

.....
.....
**The Active
Directory
Handbook**
.....
.....

comparitech

TABLE OF CONTENTS

- 1. What is Active Directory and What Can It Do?
- 2. The Basics of Using Active Directory
- 3. Forests & Domains
- 4. Create Bulk Users
- 5. Security Groups
- 6. How to Set Folder Security Permissions
- 7. The Importance of Service Accounts
- 8. How to Backup Active Directory
- 9. Our Pick of Active Directory Companion Tools

What is Active Directory?

The screenshot shows the Windows Active Directory Users and Computers management console window. The left pane displays a tree view of the directory structure under 'Active Directory Users and Computers'. The 'Users' folder is selected. The right pane is a grid view showing a list of objects with columns for 'Name', 'Type', and 'Description'. The list includes various built-in accounts and groups such as Administrator, Allowed RO..., Cert Publish..., Cloneable D..., DefaultAcco..., Denied ROD..., DnsAdmins, DnsUpdateP..., Domain Ad..., Domain Co..., Domain Con..., Domain Gue..., Domain Users, Enterprise A..., Enterprise K..., Enterprise R..., Group Polic..., Guest, Key Admins, Protected Us..., and RAS and IAS

Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
DefaultAcco...	User	A user account manage...
Denied ROD...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrato...
Enterprise K...	Security Group...	Members of this group ...
Enterprise R...	Security Group...	Members of this group ...
Group Polic...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
Key Admins	Security Group...	Members of this group ...
Protected Us...	Security Group...	Members of this group ...
RAS and IAS ...	Security Group...	Servers in this group can...

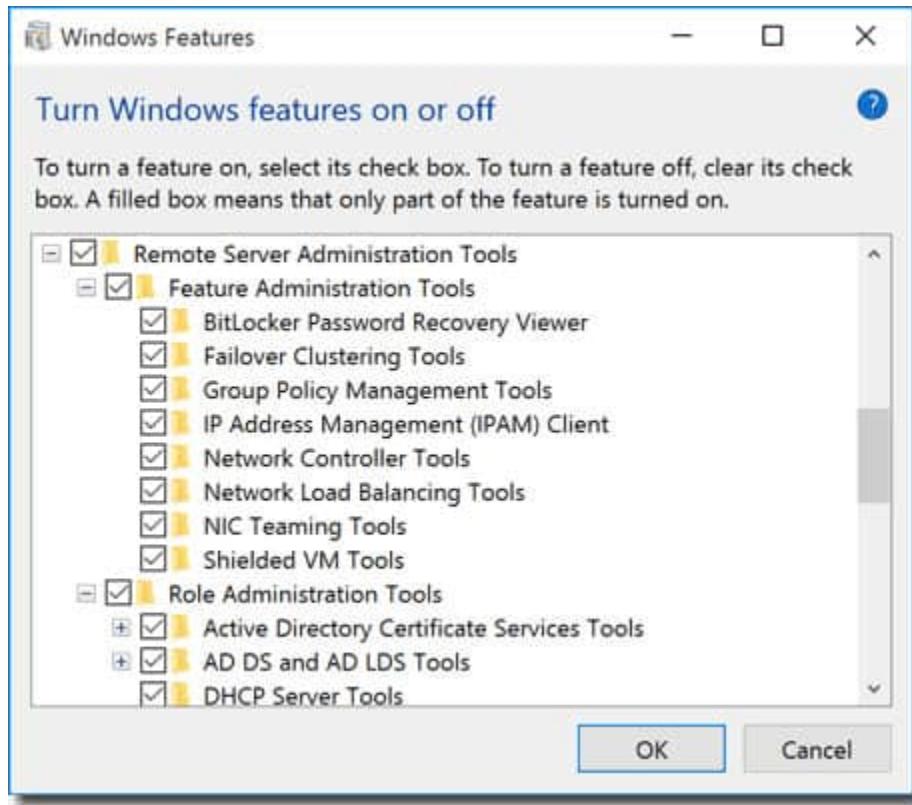
Active Directory is a directory service or container which stores data objects on your local network environment. The service records data on users, devices, applications, groups, and devices in a hierarchical structure.

The structure of the data makes it possible to find the details of resources connected to the network from one location. In essence, Active Directory acts like a phonebook for your network so you can look up and manage devices easily.

What does Active Directory do?

There are many reasons why enterprises use directory services like Active Directory. The main reason is convenience. Active Directory enables users to log on to and manage a variety of resources from one location. Login credentials are unified so that it is easier to manage multiple devices without having to enter account details to access each individual machine.

How to Setup Active Directory (with RSAT)



To begin you will need to first make sure that you have Windows Professional or Windows Enterprise installed otherwise you won't be able to install Remote Server Administration Tools. Then do the following:

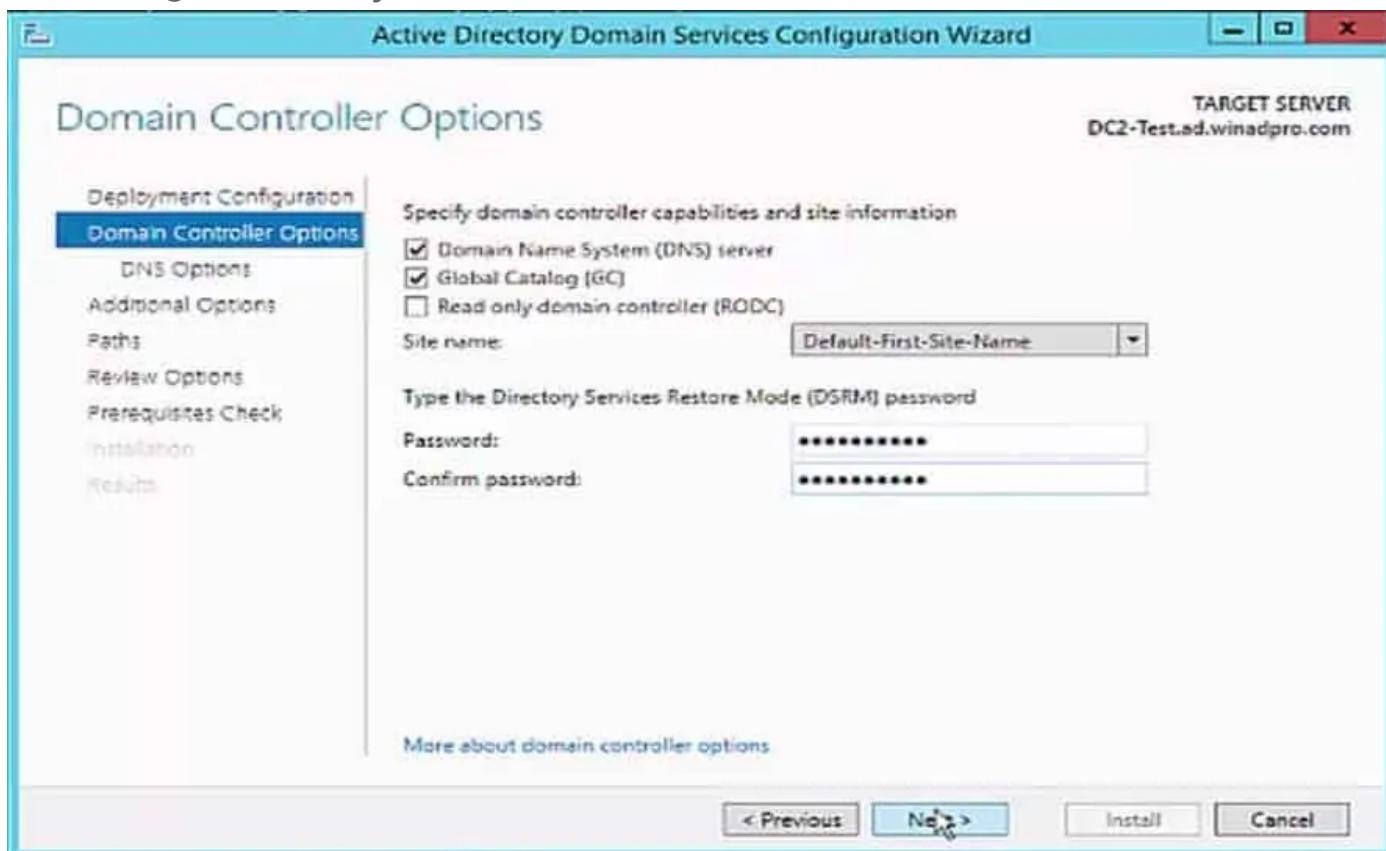
For Windows 10 Version 1809:

1. Right-click on the Start button and go to Settings > Apps > Manage optional features > Add feature.
2. Now select RSAT: Active Directory Domain Services and Lightweight Directory Tools.
3. Finally, select Install then go to Start > Windows Administrative Tools to access Active Directory once the installation is complete.

For Windows 8 (And Windows 10 Version 1803)

1. Download and install the correct version of Server Administrator Tools for your device:
[Windows 8](#), [Windows 10](#).
2. Next, right-click the Start button and select Control Panel > Programs > Programs and Features > Turn Windows features on or off.
3. Slide down and click on the Remote Server Administration Tools option.
4. Now click on Role Administration Tools.
5. Click on AD DS and AD LDS Tools and verify AD DS Tools has been checked.
6. Press Ok.
7. Go to Start > Administrative Tools on the Start menu to access Active Directory.

How to use Active Directory: How to Setup a Domain Controller, Creating Directory Users



How to Setup A Domain Controller

One of the first things you need to do when using Active Directory is to set up a domain controller. A domain controller is a central computer that will respond to authentication requests and authenticate other computers throughout the network. The domain controller stores the login credentials of all other computers and printers.

All other computers connect to the domain controller so that the user can authenticate every device from one location. The advantage of this is that the administrator won't have to manage dozens of login credentials.

The process of setting up a domain controller is relatively simple. Assign a static IP address to your Domain Controller and [install Active Directory Domain Services or ADDS](#). Now follow these instructions:

1. Open Server Manager and click Roles Summary > Add roles and features.
2. Click Next.
3. Select Remote Desktop Services installation if you're deploying a domain controller in a virtual machine or select role-based or feature-based installation.
4. Select a server from the server pool.
5. Select Active Directory Domain Services from the list and click Next.
6. Leave the Features checked by default and press Next.
7. Click Restart the destination server automatically if required and click Install. Close the window once the installation is complete.
8. Once the ADDS role has been installed a notification will display next to the Manage menu.
Press Promote this server into a domain controller.
9. Now click Add a new forest and enter a Root domain name. Press Next.
10. Select the Domain functional level you desire and enter a password into the Type the Directory Services Restore Mode (DSRM password) section. Click Next.
11. When the DNS Options page displays click Next again.
12. Enter a domain in the NetBios Domain name box (preferably the same as the root domain name). Press Next.
13. Select a folder to store your database and log files. Click Next.
14. Press Install to finish. Your system will now reboot.

Add a Domain Controller to an Existing Domain in Windows Server 2016

The procedures for **adding a domain controller** to an existing domain in Active Directory are the same, no matter which operating system you have. However, these instructions were organized during an exercise on **Windows Server 2016**. It is always a good idea to have at least two domain controllers in your AD domain just in case one goes down.

The second Domain Controller is a separate computer from the one identified for your first Domain Controller. That second computer needs to be set up with **Windows Server 2016**. Get it fully patched and assign it an IP address before starting the AD setup on that machine. Then follow these steps:

1. Open **Server Manager**, click on the **Manage** option on the menu ribbon and select **Add Roles and Features**.
2. In the opening screen of the wizard, click on **Next**.
3. In the **Installation Type** screen select the **Role-based or feature-based installation** radio button and click on **Next**.
4. In **Server Selection** leave the only server in the list highlighted and press **Next**.
5. In the **Server Roles** screen, Check the **Active Directory Domain Services** box. A dialogue box appears. Click on the **Add Features** button.
6. Back in the main feature selection screen, click the **Next** button.
7. This cycles through to the **Features** screen. Just click on the **Next** button. In the **AD DS** screen, click on the **Next** button.
8. Finally, click the **Install** button. Once the installation process finishes, you will see a notice telling you that additional steps are required. Click on the link that says **Promote this server to a domain controller**. This brings up the **Deployment Configuration** screen.
9. Leave the **Add a domain controller to an existing domain** radio button active. At the bottom of the list of options, you will see **<no credentials provided>**. Click on the **Change** button next to that.
10. Enter the username and password of the Administrator account on the AD instance that you first set up. This username should be in the format <domain>\Administrator. Click **OK**.
11. On return from the login popup, you will see that the **Domain** field has been populated with the domain that you entered for the user account. Click on the **Next** button.
12. Decide whether to make this a read-only domain controller (RODC). If so, check that box in the **Options** screen, if not, check both the **DNS server** and **Global Catalogue** boxes.
13. Enter a **DSRM password** and confirm it. Click on the **Next** button. You will see a warning but just click on the **Next** button again.
14. In **Additional Options** choose your original domain controller for the **Replicate from:** field. Click on **Next**.
15. Leave all of the paths in their default settings and click on **Next**. In the **Review Options** screen, click **Next**.
16. The system will perform a prerequisites check. If that completes satisfactorily, the **Install** button will become active. Click it.
17. Wait for the installation to complete. The computer will reboot. Log in to the machine.

Go back to your original domain controller computer and open **Active Directory Users and Computers** and you will see that your new DC is listed there in the **Domain Controllers** folder.

Creating Active Directory Users

Users and computers are the two most basic objects that you will need to manage when using Active Directory. In this section, we're going to look at how to create new user accounts. The process is relatively simple, and the easiest way to manage users is through the Active Directory Users and Computer or ADUC tool that comes with the Remote Server Administration Tools or RSAT pack. You can install ADUC by following the instructions listed below:

Install ADUC on Windows 10 Version 1809 and Higher:

1. Right-click on the Start button and click Settings > Apps, then click Manage optional features > Add feature.
2. Select RSAT: Active Directory Domain Services and Lightweight Directory Tools.
3. Select Install and wait for the installation to complete.
4. Go to Start > Windows Administrative Tools to access the feature.

Install ADUC on Windows 8 and Windows 10 Version 1803 or Lower:

1. Download and install Remote Server Administrator Tools for your version of Windows. You can do so from one of these links here:

[Remote Server Administrator Tools for Windows 10](#), [Remote Server Administrator Tools for Windows 8](#), or [Remote Server Administrator Tools for Windows 8.1](#).

1. Right-click on Start > Control Panel > Programs > Programs and Features > Turn Windows features on or off.
2. Scroll down and select Remote Server Administration Tools.
3. Expand Role Administrator Tools > AD DS and AD LDS Tools.
4. Check AD DS Tools and press Ok.
5. Go to Start > Administrative Tools and select Active Directory Users and Computers.

How to Create New Users with ADUC

1. Open the Server Manager, go to the Tools menu and select Active Directory Users and Computers.
2. Expand the domain and click Users.
3. Right-click on the right pane and press New > User.
4. When the New Object-User box displays enter a First name, Last name, User logon name, and click Next.
5. Enter a password and press Next.
6. Click Finish.
7. The new user account can be found in the Users section of ADUC.

Active Directory Events to Monitor

Like all forms of infrastructure, Active Directory needs to be monitored to stay protected. Monitoring the directory service is essential for preventing cyber-attacks and delivering the best end-user experience to your users.

Below we're going to list some of the most important network events that you should look out for. If you see any of these events then you should investigate further ASAP to make sure that your service hasn't been compromised.

An Overview of Active Directory Forests and Trees

Forest and trees are two terms you will hear a lot when delving into Active Directory. These terms refer to the logical structure of Active Directory. Briefly, a tree is an entity with a single domain or group of objects that is followed by child domains. A forest is a group of domains put together. When multiple trees are grouped together they become a forest.

Trees in the forest connect to each other through a trust relationship, which enables different domains to share information. All domains will trust each other automatically so you can access them with the same account info you used on the root domain.

Each forest uses one unified database. Logically, the forest sits at the highest level of the hierarchy and the tree is located at the bottom. One of the challenges that network administrators have when working with Active Directory is managing forests and keeping the directory secure.

For example, a network administrator will be tasked with choosing between a single forest design or multi-forest design. The single-forest design is simple, low-cost and easy to manage with only one forest comprising the entire network. In contrast, a multi-forest design divides the network into different forests which is good for security but makes administration more complicated.

Trust Relationships (and Trust Types)

As mentioned above, trusts are used to facilitate communication between domains. Trusts enable authentication and access to resources between two entities. Trusts can be one-way or two-way in nature. Within a trust, the two domains are divided into a trusting domain and a trusted domain.

In a one-way trust, the trusting domain accesses the authentication details of the trusted domain so that the user can access resources from the other domain. In a two-way trust, both domains will accept the other's authentication details. All domains within a forest trust each other automatically, but you can also set up trusts between domains in different forests to transfer information.

You can create trusts through the New Trusts Wizard. The New Trust Wizard is a configuration wizard that allows you to create new trust relationships. Here you can view the Domain Name, Trust Type, and Transitive status of existing trusts and select the type of trust you want to create.

How to Find the Source of Account Lockouts in Active Directory

The easiest way to find account lockouts in Active Directory is to use the Event Viewer, which is built into Windows. Active Directory generates Windows Events messages for each of its actions, so your first task is to track down the right event log.

1. Open a PowerShell window by pressing the Windows key and R together. In the Run popup, type **powershell** and hit ENTER.
2. At the command line type **(get-addomain).pdcemulator**
3. Note down the address of the PCD Emulator domain controller, which will be shown on the next line.
4. Type **exit** to close the PowerShell window.
5. The standard event log viewer that is built into the Windows operating system will help you find the account lockouts.
6. Go to the DC named as the PDC Emulator.
7. Open the Event Viewer by expanding **Windows Administrative Tools** in the Start menu and clicking on the **Event Viewer** entry in that submenu.
8. In the Event Viewer, expand the **Windows Logs** node in the left-hand menu tree. Click on **Security**. The Security events list will appear in the central panel of the Event Viewer.
9. In the right panel of the Event Viewer, click on **Filter Current Log**, which will open a popup window.
10. In the **Event IDs** field replace <All Event IDs> with **4740**.
11. Select a time horizon in the **Logged** drop-down list at the top of the form.
12. Optionally, enter a username or a hostname if you are specifically looking for a lockout on a specific user or resource.
13. Press **OK**.
14. Double click on the log entry that relates to the user or resource that interests you and that has a timestamp that matches the moment you think the lockout occurred. This will open the Event Report.

The Event Report will show you the user that was locked out, the computer that the event occurred on, and the source, or reason for the lockout.

Active Directory FAQs

What is the difference between an Active directory and a Domain controller?

Active Directory is an authentication system. A **domain** is a collection of objects, which are users, computers, and devices that all have access rights managed in the same Active Directory database. The **domain controller** is the authentication management system that implements Active Directory functions on the domain's database objects.

How to enable the Security Auditing of Active Directory?

In order to start security auditing within Active Directory:

1. Log in to **Windows Server** as an administrator.
2. Go to **Start**, click on **Administrative tools**, and select **Group policy management console**.
3. Get to the **domain/OU** to be audited.
4. Right-click on the **Group Policy Object**, and choose **Edit**. This will open the Group Policy Management Editor.
5. In the left-hand tree menu, expand **Computer Configuration**, then **Policies**, expand **Windows Settings**, then **Security Settings**, and finally **Local Policies**. Click on **Audit Policies**.
6. In the main panel of the Editor, click on **Audit object access** and select both the **Success** and **Failure** options.
7. Click on **Audit directory service access** and select both the **Success** and **Failure** options.

What is the difference between Active Directory and LDAP?

The Lightweight Directory Access Protocol (LDAP) is an open standard that outlines how access rights can be managed. Active Directory is an access rights management system, written by Microsoft. Active Directory is an evolution of the concepts defined in LDAP.

What are Active Directory and Single sign-on and what are the differences between them?

Single sign-on (SSO) gives each user access to several systems with just one authentication procedure. Active Directory (AD) is an access rights management system that can implement an SSO environment.

Can I install Active Directory on client operating systems?

No. Active Directory is a server function and it is integrated into the Windows Server operating system. Logically, any client running Active Directory would become a server.



Domains, trees, and forests

The concept of a domain is commonly understood by the networking community. A website is a domain and is identified on the World Wide Web by a domain name. Another use of the term lies in addressing on a network where all computers are within the same address space, or '**scope**'.

In Active Directory terminology, a domain is the area of a network covered by one single authentication database. The store of that database is called a **domain controller**.

Several domains can be linked together in a **tree structure**. So, you can have a **parent domain** with **child domains** linked to it. The child domains inherit the address space of the parent, so the child is a subdomain. The top of the tree structure is the **root domain**. The whole group of parents and child relationship forms the tree. A child to one domain can also be the parent to other domains.

So, think of a group of domains that share the same root domain address as a tree. Once you can see the trees, you can work out what the forest is: **it is a collection of trees**.

Distribution and replication

The concept of a forest is complicated slightly by the fact that it is a collection of unique trees. On large networks, it is a common practice to **replicate the domain controller** and have several copies on different servers around the system – this speeds up access.

If you operate a multi-site WAN you want to have a common network access system for the whole organization. The location of the domain controller can have a **serious impact on performance**, with users at remote locations having to wait longer in order to log into the network. Having copies of the domain controller locally gets around this problem.

When you have several copies of the same domain controller in different locations, you don't have a forest.

The central administration module of Active Directory **needs to coordinate all of the copies** to make sure all of the databases are exactly the same. This requires a process of replication. Although the Active Directory permissions database is distributed around the network, it is not what is officially regarded as a '**distributed database**'. In a distributed database, the collection of records is split between several servers. So, you would need to visit each server in order to gather the full database. This is not the case with Active Directory because each server (domain controller) has **an exact and complete copy of the database**.

Benefits of replication

A replicated domain controller has several **additional benefits for security**. If one domain controller gets damaged accidentally, you can replace all of the original records by copying over the database from another site. If a hacker gets hold of credentials from one of the users on a network, he may try to alter the permissions held in the local domain controller to get high privileges, or wider access to resources on the network. Those changes can be rolled back once spotted.

The constant comparison on domain controller databases provides a key security measure. The replication process can also help you **shut down a compromised account** all across the system. However, the restoration of an original database and the roll out of updated records requires very regular system sweeps and integrity checks in order to be effective.

The management of replication is a key task for network managers operating Active Directory. The fact that there can be many local domain controllers **can give intruders an opportunity to sneak around a segment of the network and steal or alter data** before being detected and locked out. The coordination between copies of domain controllers can soon become a very complicated and time-consuming task. **It cannot be carried out manually within a reasonable timeframe.** You need to use automated methods to keep frequent checks on all domain controllers and to update all servers when a change is made to the permissions that they contain.

Defining a forest

In order to have a forest, you need to have several domain trees. This scenario could exist if you want to have **different permissions for different areas of your network**. So, you might have a separate domain per site, or you might want to keep the permissions for certain resources or services on your network completely separate from the regular network authentication system. So, domains can overlap geographically.

Your company network may contain **many domain controllers** and some of them will all contain the same database, while others contain different permissions.

Imagine your company runs services for users on its own network and wants to **keep those permissions separate** from the resources accessed by staff. It would create two separate domains. If you also run Exchange Server for your company email system, you will have another AD domain.

Although the staff email system will probably have the same domain name as the website, you do not HAVE to keep all domains with the same domain root in the same tree. So, the email system can have a single-domain tree and the user network can have a separate single-domain tree. So, in this scenario, you are dealing with three separate domains, which make a forest.

The Exchange domain may well have just one domain controller, because the actual server for the email system is only resident in one location, and so only needs to access one authentication database. The user domain might only need to be in one location – on the gateway server. However, **you could implement an instance of your staff domain controller for each of your company's sites.** So, you may have seven domain controllers, five for the staff domain, one for the user domain, and one for the email domain.

You might want to divide up the internal network into subsections by office function, so you would have an accounts section and a sales section with no interoperability. These would be two child domains of the parent staff domain, forming a tree.

One reason to keep the staff network separate from the user network is for security. The need for privacy on the internal system may even extend to **creating a separate domain name for that staff network**, which does not need to be made known to the general public. This move forces the creation of a separate tree because you cannot have different domain names included in one tree. Although the email system and the user access system only have one domain each, they also each represent a tree. Similarly, if you decided to create a new website with **a different domain name**, this could not be merged into the administration of the first site because it has a different domain name.

Splitting up the staff domain to create child domains requires more domain controllers. Rather than just one domain controller per site for the staff network, you now have three per site, making a total of 15 over five sites.

Those 15 staff domain controllers need to be replicated and coordinated with the tree structure relationship between the three original domains preserved on each of the five sites. Each of the other two domain controllers are distinct and **won't be part of the replication procedures** of the staff domain. The site has three trees and one forest.

As you can see from this relatively simple example, the complexity of managing domains, trees, and forests can quickly become unmanageable without a comprehensive monitoring tool.

Global Catalog

Although the separation of resources into domains, subdomains, and trees can enhance security, it doesn't automatically eliminate the visibility of resources in a network. A system called **Global Catalog (GC)** lists all of the resources in a forest and it is replicated to every domain controller that is a member of that forest.

The protocol that underpins GC is called the '**transitive trust hierarchy**.' This means that all elements of the system are assumed to be bona fide and not harmful to the security of the network as a whole. Therefore, the authentication records entered in one domain can be trusted to grant access to a resource that is registered on another domain.

Users given permissions to resources in one domain don't automatically get access to all resources, even within the same domain. The GC feature that makes resources visible to **all** does not mean that **all users can access all resources in all domains of the same forest**. All that GC lists is the name of all objects in the forest. It isn't possible for members of other domains to query even the attributes of those objects in other trees and domains.

Multiple forests

The forest isn't just a description of all trees run by the same administration group, there are common elements for all domains that are held at forest level. These common features are described as a '**schema**.' The schema contains the design of the forest and all of the domain controller databases within it. This has a unifying effect, which is expressed in the common GC that is replicated to all controllers within the same forest.

There are some scenarios where you might need to maintain **more than one forest** for your business. Because of GC, if there are resources that you want to keep completely secret from members of the domains, you would have to create a separate forest for them.

Another reason that you might need to set up a separate forest is if you are installing AD management software. It could be a good idea to create a sandbox copy of your AD system to try out the configuration of your new software before letting it loose on your live system.

If your company acquires another business that already operates Active Directory on its network, you will be faced with a number of options. The way your business deals with the new company will dictate how you operate the network of that new division. If the business of the new company is going to be taken over by your organization and the name and identity of that company will be retired, then **you will need to migrate all of the users and resources of the acquired business over to your existing domains, trees, and forest.**

If the acquired company will carry on trading under its existing name, then **it will be continuing with its current domain names**, which cannot be integrated into your existing domains and trees. You could port the trees of this new division over to your existing forest. However, a simpler method is to leave that acquired network as it is and link together the forests. It is possible to **create a transitive trust authority between two independent forests**. This action must be performed manually and it will extend the accessibility and visibility of resources so that effectively, the two forests merge on a logical level. You can still maintain the two forests separately and that trust link will take care of mutual accessibility for you.

Active Directory Federation Services

Active Directory runs a number of services that **authenticate different aspects of your system** or aid cohesion between domains. One example of a service is the **Active Directory Certificate Services** (AD CS) which controls public key certificates for encryption systems, such as Transport Layer Security. The service that is relevant to domains and forest is the **Active Directory Federation Services** (AD FS).

AD FS is a single sign-on system, which extends the authentication of your network out to services run by other organizations. Examples of systems that can be included in this service are Google G-Suite facilities and Office 365.

The **single sign-on system** exchanges authentication tokens between your AD implementation and the remote service so once users have logged into your network, they will not need to log in again to the participating SSO remote service.

Managing AD forests and domains

A relatively straightforward structure for Active Directory can quickly become unmanageable once you start creating subdomains and multiple forests.

Generally, **it is better to err towards having as few domains as possible**. Although separating out resources into different domains and subdomains has security benefits, the increased complexity of a multiple-instance architecture can make intrusion tracking difficult.

If you are beginning a new Active Directory implementation from scratch, it is recommended that you **start off with one domain in one tree**, all contained by one forest. Select an AD management tool to assist you in the installation. Once you have become adept at managing your domain with your chosen tool, you can consider splitting out your domain into subdomains and also adding on more trees or even forests.

```
# Import Active Directory module for running AD cmdlets
Import-Module activedirectory

#Store the data from ADUsers.csv in the $ADUsers variable
$ADUsers = Import-Csv

#Loop through each row containing user details in the CSV file
Foreach ($User in $ADUsers)
{
    #Read user data from each field in each row and assign the data to a variable as below
    $Username = $User.username
    $Password = $User.password
    $FirstName = $User.firstname
    $LastName = $User.lastname
    $OU = $User.OU
    $Email = $User.email
    $StreetAddress = $User.streetaddress
    $City = $User.city
    $Zipcode = $User.zipcode
    $State = $User.state
    $Country = $User.country
    $Telephone = $User.telephone
    $JobTitle = $User.jobtitle
    $Company = $User.company
    $Department = $User.department
    $Password = $User.Password
}
```

Ultimate Guide

Create Bulk Users in Active Directory

comparitech

Active Directory (AD) is used by 95 percent of US Fortune 500 companies. It is the leading identity and access management system in the USA and it is taking on big rivals by strengthening its lead through cloud deployment with the Azure platform.

As a system administrator, it is highly likely that you are going to get to know AD really well. The pressure for greater efficiency and the squeeze businesses always put on IT budgets makes it difficult to argue for funds to acquire specialized IT tools to **automate mundane tasks**. So, you end up implementing manual tasks to provide the time-saving systems that everyone else in the business can enjoy.

Fortunately, the procedures to bulk create new accounts in Active Directory with just the software you already have is not too difficult. We will show you how. We will also look into some free tools that you can get in order to perform this task if you just don't have the time to study PowerShell commands.

Hint: Uploading new users into PowerShell is a lot easier with a free tool than it is with PowerShell.

Prepare Active Directory

If you are using Active Directory, you probably already have all of the necessary tools available on your server. However, just to be sure, look at the following steps.

1. Go to the Start menu and click **Server Manager**. This should open a new window.
2. In the **Server Manager Dashboard**, select **Add roles and features**.
3. In the **Before You Begin** screen, click **Next**. In the **Select installation type screen**, make sure **Role-based or feature-based installation** is selected, and then press **Next**.
4. In **Select destination server**, click **Next** to select your local server. This displays the **Add Roles and Features** screen.
5. Select **Server Roles** in the left-hand menu and make sure that the **Active Directory Domain Services** role is checked. If you are just starting up a new Active Directory installation you will need to activate this role, if you are already running Active Directory, this role will already be running.
6. Click **Features** in the left-hand menu. Make sure that **Remote Server Administration Tools** is checked. Expand this node and ensure that **AD DS and AD LDS Tools** is checked. If they are, you are good to go; if not, check it and click to install the option.

Also, in the **Add roles and features** screen, you can make sure that you have the PowerShell ISE service working. Click **Features** in the left-hand menu and scroll down through the list in the main panel of the screen. Click **Windows PowerShell** to expand that node and make sure that **Windows PowerShell ISE** is checked. If not, click this option and install it.

Set up user account details

Now that you have made sure that all of the PowerShell utilities you need are running on your server, you can create a list of all of the accounts that you want to upload. Open your favorite spreadsheet system and create a new file.

Make a heading line and in columns A to E type in the headings firstname, lastname, username, password, email, streetaddress, city, zipcode, state, country, telephone, jobtitle, department, company, and OU. Enter a record for each account that you want to create. If you don't have data for all of the columns, you can leave those fields blank except for firstname, lastname, username, password, and OU, which must have values.

The OU column gives the details of the Organizational Unit. You should have these set up already in Active Directory, they are the departments or business functions that you assign to each user account.

In order to see exactly what value to put in this column:

1. Open **Active Directory Users and Computers**.
2. Select your Active Directory instance, select **View** in the top menu, and click **Advanced Features**.
3. Right-click the organizational unit that you want to assign a user to and click **Properties**. Select the **Attribute Editor** tab.
4. Double click the **distinguishedName** line. This will open a popup window. You can copy the attribute value from here and paste it into the OU field for the new user account record that you are creating in your spreadsheet.

Once you have entered records for all of the accounts you want to load, save the spreadsheet. Start to save the spreadsheet again, but this time, use the **Save As** option. Select **CSV** as the file type. You can make changes in the spreadsheet version and use the CSV version for the bulk upload. Remember, whenever you make changes to the spreadsheet, you need to generate a new version of the CSV file in order to get those changes written to your import file.

Create a PowerShell script

Open a text editor, such as Notepad in order to create a PowerShell script to import your list of users.

Copy the following text and paste it into the new file:

```

# Import Active Directory module for running AD cmdlets

Import-Module activedirectory

#Store the data from your file in the $ADUsers variable

$ADUsers = Import-csv <fileandpath>

#Loop through each row containing user details in the CSV file

foreach ($User in $ADUsers)
{
#Read user data from each field in each row and assign the data to a variable as
below
$Username = $User.username
$Password = $User.password
$Firstname = $User.firstname
$Lastname = $User.lastname
$OU = $User.ou
$email = $User.email
$streetaddress = $User.streetaddress
$city = $User.city
$zipcode = $User.zipcode
$state = $User.state
$country = $User.country
$telephone = $User.telephone
$jobtitle = $User.jobtitle
$company = $User.company
$department = $User.department
$Password = $User.Password

#Check to see if the user already exists in the AD

if (Get-ADUser -F {SamAccountName -eq $Username})
{
#If the user does exist, give a warning
Write-Warning "A user account with username $Username already exists in Active
Directory."
}
else
{
#User does not exist then proceed to create the new user account
#Account will be created in the OU provided by the $OU variable read from the CSV
file
New-ADUser `

-SamAccountName $Username `

-UserPrincipalName "$Username@<domain>" `

-Name "$Firstname $Lastname" `
```

```
-GivenName $Firstname `  
-Surname $Lastname `  
-Enabled $True `  
-DisplayName "$Lastname, $Firstname" `  
-Path $OU `  
-City $city `  
-Company $company `  
-State $state `  
-StreetAddress $streetaddress `  
-OfficePhone $telephone `  
-EmailAddress $email `  
-Title $jobtitle `  
-Department $department `  
-AccountPassword (convertto-securestring $Password  
-AsPlainText  
-Force)  
-ChangePasswordAtLogon $True
```

```
}  
}
```

***** End of script - do not copy this line ***

There are two elements in the above script that you need to customize before you run it. These are:

- <fileandpath> Replace this with the file name of your CSV file, including the .csv extension and the full path all the way from the root, including the drive letter. For example, C:\Users\Administrator\Documents\users.csv
- <domain> Replace this with the domain name of your AD server.

Once you have created the PowerShell script, **save it**. Give the script a name that has the extension **ps1** – for example uploadusers.ps1.

Import users in AD with PowerShell

1. Open File Explorer and click the directory where you saved your PowerShell script.
2. Right-click the script and select **Edit** from the context menu. This will open **Windows PowerShell ISE**.
3. Look for a green play icon in the button bar at the top of the screen and press it. If any of the accounts that you tried to upload already exist in your AD directory, you will see a warning message for each duplication – the duplicate record will not be entered into the database. When the script finishes its work, the PowerShell prompt will reappear.
4. Go back to **Active Directory Users and Computers**. Click each of the departments that you created new user accounts for and check that all of the accounts that you held in the CSV file have actually been created.

An automated tool for uploading accounts into AD

If you are uncomfortable with running PowerShell scripts, you might be happier with a well-designed tool with an attractive GUI interface instead. You probably already use a lot of different tools in your job administering the company IT system, so this strategy will be easy to understand.

The big advantage that PowerShell has over third-party systems is that you already have it and you don't have to pay for it. In many companies, requirements laid down to justify buying a new tool can be off-putting. However, there are some really good free tools for the bulk creation of Active Directory user account. That removes the need to seek budgetary approval.

[SolarWinds Admin Bundle for Active Directory \(FREE TOOL\)](#)

Take a look at the [Admin Bundle for Active Directory](#) which is totally free forever – it isn't a trial. The bundle is provided by SolarWinds and it has a great user interface. It measures up to the high standards that SolarWinds uses for its paid system monitoring and management tools.

There are three separate tools included in this package. These are the **Remove Inactive Users** utility, the **Remove Inactive Computers** tool, and the **User Import Tool**. Of the three, it is the third one that we will look at here.

Download and install the User Import Tool

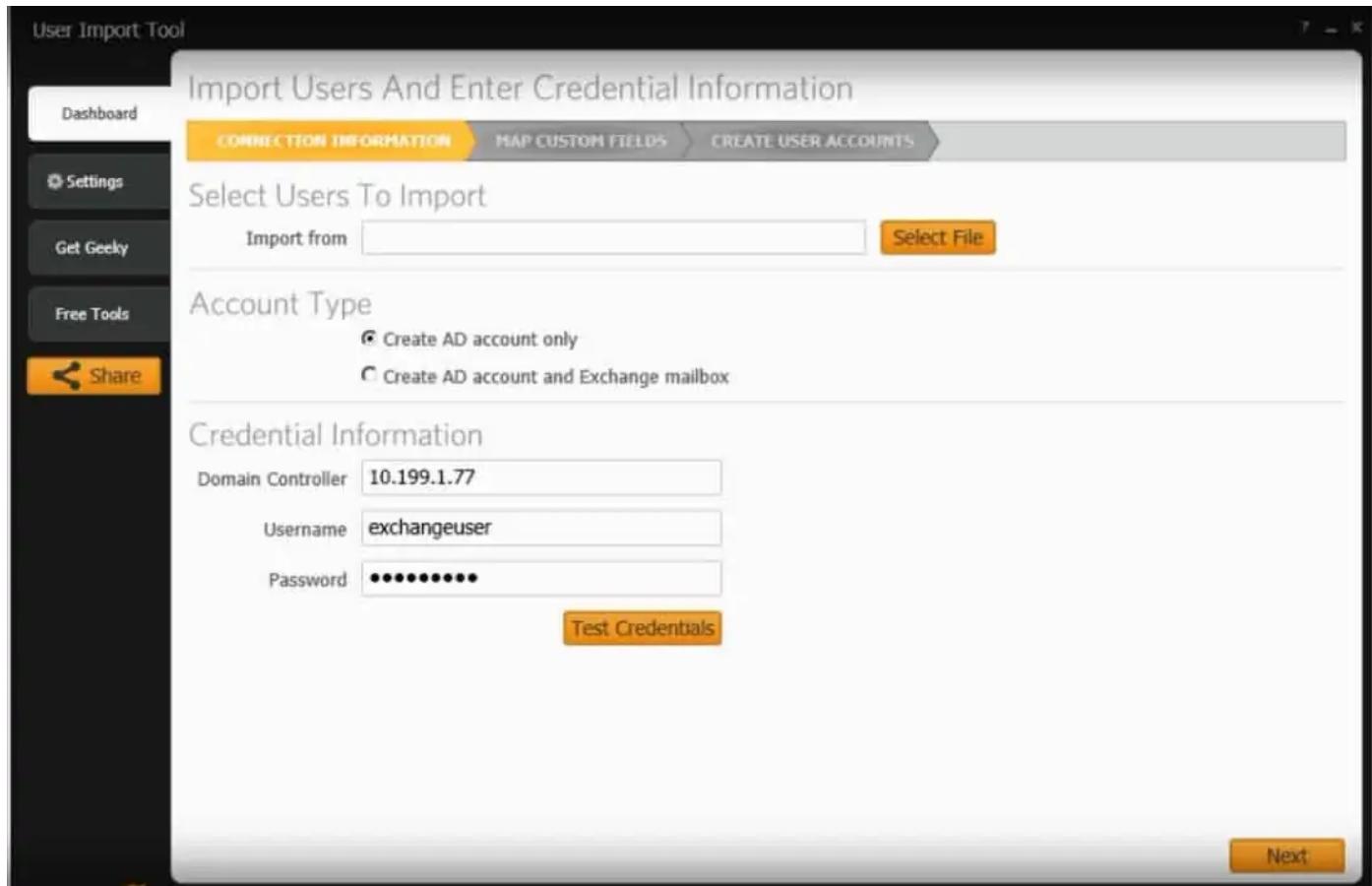
Access the Create User Account utility at the [Admin Bundle for the Active Directory download page](#). This will download an installation Wizard. Click the downloaded file to start the installation process.

Cycle through the installation instructions to get the utilities installed on your device. The bundle will install on Windows as well as Windows Server. The three utilities are created as separate tools – they are not accessed through a unified portal.

[Admin Bundle for Active Directory Download 100% FREE Tool](#)

Bulk create accounts with the User Import Tool

Once the installation has completed, find the **User Import Tool** in the Start menu. This system will import a file created with a spreadsheet. So, you would create a list of new users in exactly the same way as the process described in the section for creating users through a PowerShell script. In the case of the User Import Tool, however, it is not necessary to save your spreadsheet in a **CSV format** if you use Microsoft Excel. This is because this utility will accept **XLSX files** as well as CSV files for input.



The first time you use the service you will need to enter the **login credentials** of your Active Directory administrator account. However, these are stored when you close the utility, so they will be available for your next session.

After entering the administrator account details, click the **Test Credentials** button. This will create a connection to the Active Directory instance.

The utility will create entries for the new users you want to upload in an associated Microsoft Exchange instance, generating mailboxes for each new account. If you want to activate this option, click the **Create AD account and Exchange mailbox** radio button. The top field in the Home screen of the User Import Tool is for the path and name of the input file. You can locate this through a file explorer by clicking the **Select File** button. Once all the fields on the screen have been filled in, click the **Next** button to proceed.

In the next screen, the tool displays the column headings it discovered in the input file and suggests some attributes in the AD system that might match.

User Import Tool

Map Custom Fields

CONNECTION INFORMATION MAP CUSTOM FIELDS CREATE USER ACCOUNTS

Select an item from each list and click 'Map Attribute' to create a mapping between the file column and the account attribute.

From:

First Row Fields	
user	
email address	
department	
phone number	

To:

Field	Mapped From
Sam-Account-Name	
Password	
OrganizationalUnit	

Map Attribute
Clear Map
Default Map

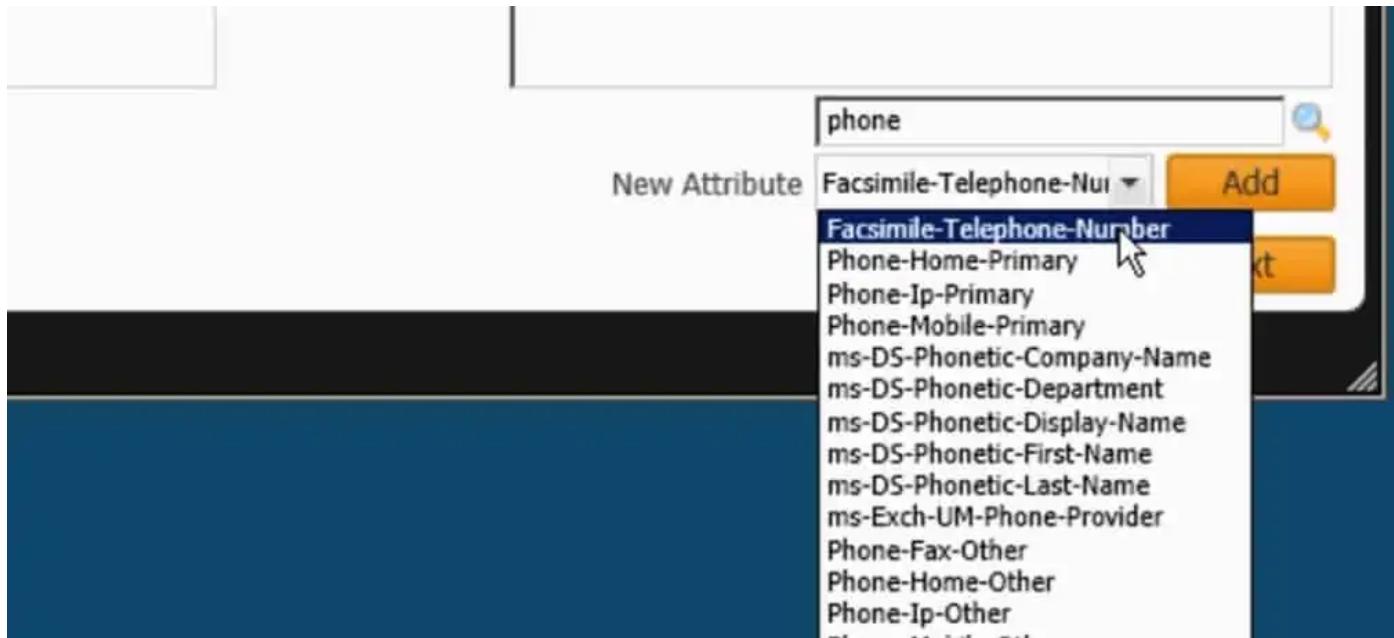
Import First Row

New Attribute Common-Name Add

Back Next

You can add attributes to the right column of the screen by typing a field name in the search field below that panel and then scrolling through the list of results.

Click an attribute to get it in the candidate field and then click the **Add** button to get it in the list of available attributes.



Next, you click a column name in the list of input file headings and then click the related attribute name from AD in the right column. With both fields highlighted, press the **Map Attribute** button. This links the column to the attribute. Click the **Next** button after mapping all of the columns.

The next screen shows a preview of all of the records that are going to be added to the Active Directory. Click the **Create** button to get those records imported.

Go to the **Active Directory Users and Computers** screen from the Start menu to check that those new user accounts are now in the system.

Bulk importing Active Directory accounts

Whether you choose to copy the **PowerShell script** shown here to import users or access the free **User Import Tool** from SolarWinds, creating users through a spreadsheet is a useful way to add a lot of users all at once. Creating a list in a spreadsheet outside the AD system enables you to build up a list over time and you don't feel so pressured to type in all of the account details in one session.



The image features a white smartphone-like device centered against a blue and teal background. On the screen of the device is a graphic of a blue and yellow 3D pyramid with a yellow shield containing a black lock icon in front of it. Below the device, the words "Ultimate Guide" are written in a large, dark grey sans-serif font. To the right of the device, the title "AD Security Groups" is displayed in a large, white, sans-serif font. In the bottom right corner of the slide, the "comparitech" logo is visible.

AD Security Groups

Ultimate Guide

comparitech

AD Security Groups and Permissions

Active Directory group management is the classifying and managing of users and devices across a network by bundling them together into AD groups.

AD security groups enable network administrators to manage permissions, policy settings, and group access to shared resources among a collection of users or devices all at once, rather than manually assigning permissions to individual users one at a time. For instance, if you want to grant staff in the HR department access to a specific network folder, you need to create a security group made up of staff from that unit.

This simplifies network administration by allowing you to assign permissions once to multiple users. Users can be added or removed from the group as the need arises. The change in group membership automatically takes effect everywhere. With AD security groups, network admins can:

- Assign user rights: User rights can be assigned to a security group. This helps to control what the users within the group can or cannot do within a domain or forest. For some security groups, user rights are automatically assigned for administration purposes which in turn can be inherited by members of the group. It's critical that you pay special attention to those automatically assigned user rights to ensure that they are within required boundaries.

- Assign permissions for resources. User permissions are distinct from user rights. Rights define the capabilities users possess, whereas permissions relate to access to resources. Some security groups are created by default and permissions automatically assigned when you create an Active Directory domain. Again extra care must be taken in managing those types of groups due to their automatic security permissions.

When assigning permissions for resources (such as network folders, printers), it is best practice to assign those permissions to a security group rather than to individual users. Members of a security group inherit rights and permissions assigned to that group in Active Directory.

Active Directory groups (including security groups) are characterized by their scope. The scope of the group determines the extent to which the group is applied in the domain tree or forest, and defines where the group can be granted permissions. The following three group scopes are defined by Active Directory:

1. Domain local: Domain local manages access permissions to different domain resources (such as files and [folders NTFS permissions](#), remote desktop access, etc.) in the domain where it was created; and can be applied anywhere in the domain. A domain local group can include members from trusted domains or other types of members.
2. Global: The global group scope is used to provide access to resources in another domain. Global groups are usually used as role-based groups; which means that domain objects (such as users and computers) are defined based on business roles.
3. Universal: Just as the name implies, with the universal group scope, you can define roles and manage access to resources that are distributed across multiple domains in a forest.

AD Security Groups Best Practices

Active Directory security groups include Administrators, Domain Admins, Server Operators, Account Operators, Users, Guests, among others. A good understanding of how to manage these security groups with a best-practice mindset is key to keeping your system secure. The following are key AD security groups best practices:

- Ensure default security groups don't have excessive permissions: Regularly [audit permissions](#) automatically assigned by default security groups when you set up an Active Directory domain, as some of these groups have extensive permissions. Ensure that users only have just enough access rights required to carry out their daily tasks and nothing more. If higher access rights are required, it should be provided on a temporary basis as and when needed.
- Keep software regularly updated: Ensure that your Windows software and other third-party applications are regularly updated. Attackers often exploit or take advantage of known vulnerabilities to compromise systems. Regular patching can help minimize this risk.
- Good password policy: Implement [password policies](#) that encourage users to use passphrases they can easily remember instead of focusing on complexity rules. Complexity rules make passwords harder to remember, and most users end up writing them down, which defeats the whole purpose in the first place. It's also recommended to set rules that lockout users after several failed login attempts. Adopt the use of Windows supported [2FA/MFA](#) such as Windows Hello or FIDO for extra protection.
- Maintain a policy of zero trust: [Zero trust](#) means that no one is trusted by default from inside or outside the network, and verification is required from everyone trying to gain access to resources on the network. Insider threat is a risk no organization should underestimate because it can be incredibly difficult to track the source. Adhere to the principle of least privilege access to network resources and ensure that users don't have excessive permissions.
- Audit changes to AD Security groups: Auditing helps to detect anomalous user behavior and system events. AD related security vulnerabilities and threats can potentially be prevented through better visibility into changes that take place within the security group. Having a good auditing strategy for your AD security groups is a sure way to prevent security threats. Changes to privileged groups should be alerted in real-time to ensure that you can investigate the change and revert it if excessive permissions were created.

5 Best Tools for Managing AD Security Groups

1. SolarWinds Permissions Analyzer FREE TOOL: One of the common challenges with the Microsoft Active Directory program is that it offers poor permissions management. This is where SolarWinds Permissions Analyzer stands out. [SolarWinds Permissions Analyzer](#) enables network admins to gain better visibility into user and group permissions, check permissions assigned on Active Directory objects, browse permissions by a group or user, or analyze user permissions based on group membership and permissions even in multi-domain Active Directory Forest. Some of the key features and capabilities include:

- Identify how a user's permissions are inherited
- Browse permissions by group or individual user
- Analyze user permissions based on group membership and permissions



Figure 1.0 Screenshot showing SolarWinds Permissions Analyzer interface

Imagine an insider threat scenario where an employee gains excessive rights to key company resources and suddenly begins to carry out malicious activities from the inside. You observe that this employee has access to all sorts of key company groups, shared network folders, and files; but nobody is fully sure what and how much. This could be a major security issue for your organization, so you need to get to the root of what's going on quickly. One way to investigate this is to use PowerShell if you have the skill and experience to do it, but the reality is that not everyone does. That's where SolarWinds Permissions Analyzer comes into play. With this tool, network admins can easily identify which members of their team have access privileges to sensitive data.

Best of all, SolarWinds Permissions Analyzer is available for [download free of charge](#).

[Permissions Analyzer for Active Directory Download 100% FREE Tool](#)

2. SolarWinds Access Rights Manager (ARM) FREE TRIAL: SolarWinds ARM is designed to assist IT and security administrators in managing and regulating user access rights and permissions to systems and data across domains, which is an important step in protecting the organizations from cyber risks. Its auditing and permissions management capabilities make it easy to analyze user authorizations, access permissions and Group Policy to give you better visualization of who has access to what, and how and when they accessed it.

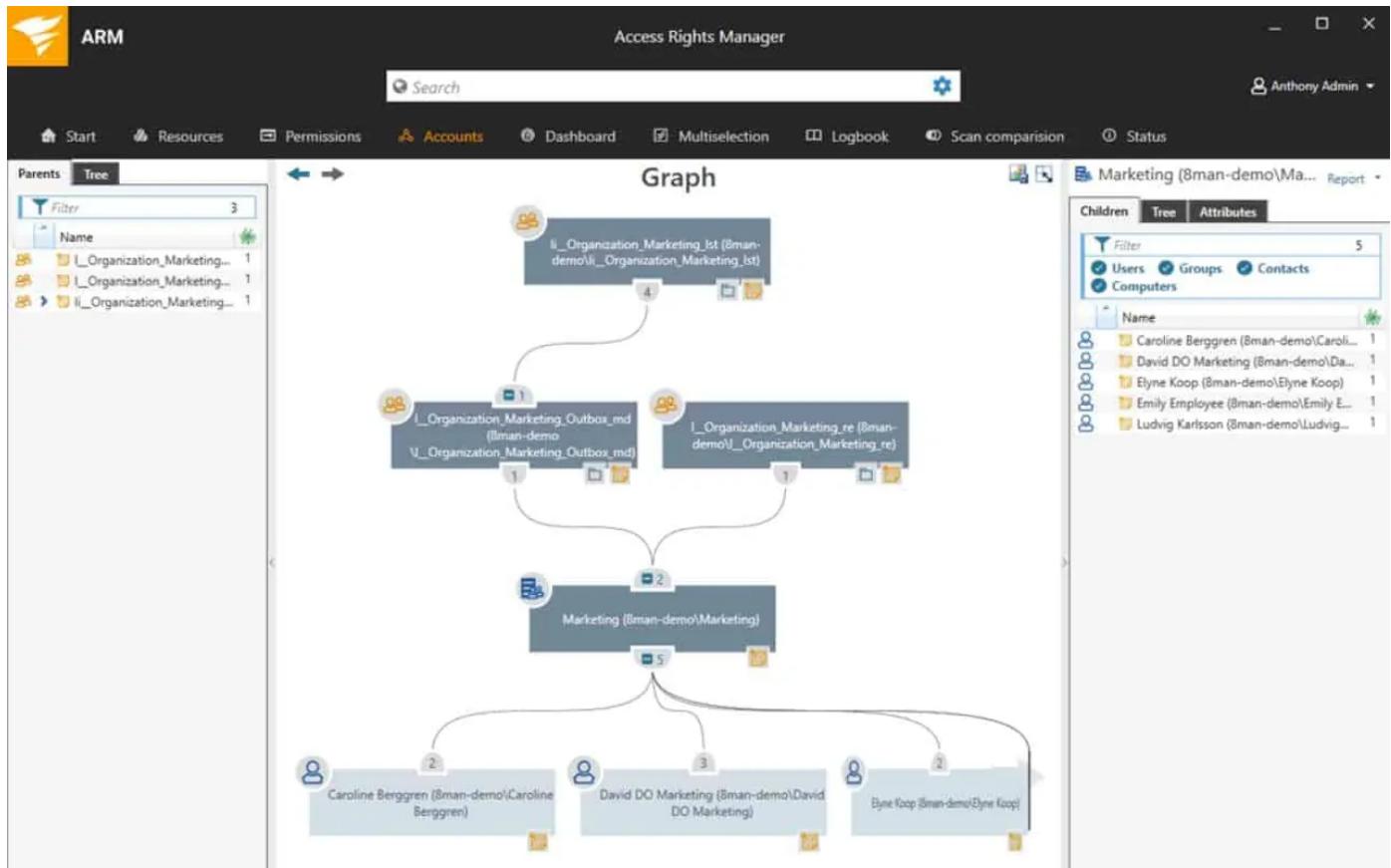


Figure 2.0 Screenshot showing SolarWinds ARM dashboard

The custom report generation features allow for the quick creation of a variety of AD reports, from simpler reports for management to more technical and detailed reports appropriate for auditors.

SolarWinds ARM enables network admins to perform the following access rights management activities:

- Permission Analysis: This feature helps admins to define which users have access to which data. Some of the key activities that can be performed include: view permission settings, track access paths, understand nested group permissions, among others.
- User Provisioning: User provisioning helps admins to create and manage user accounts and groups.
- Security Monitoring: Security monitoring empowers network admins to leverage logs from across Active Directory, file servers, and other systems and tools to generate reports, alerts, and track key activities.
- Role and Process Optimization: This feature enables network admins to automate the process of determining data owners across business units and departments. Data owners play a key role in determining and defining user access rights and permissions.

[SolarWinds Access Rights Manager Download 30-day FREE Trial](#)

3. ManageEngine ADManager Plus: **ADManager Plus** is web-based AD management and reporting tool that provides centralized administration and management of Windows Active Directory. It allows IT admins to manage AD objects and groups from one central location via a user-friendly GUI. Network admins can use ADManager Plus to perform the following functions:

- Generate and view granular reports of users, computers, groups such as Inactive Users, Disabled Users, Users in Nested Groups, Distribution Groups, Security Groups, Inactive Computers, among others.
- Modify the existing user account properties including Exchange Mailbox and Terminal Services properties.
- Create bulk user accounts in the Active Directory with the flexibility to import properties from a CSV file.
- Create and delegate security roles for granting/revoking permissions to security principals.

The screenshot shows the ADManager Plus dashboard. At the top, there's a header with the logo, user info (Welcome, admin), and navigation links like Home, AD Mgmt, AD Reports, AD Delegation, Workflow, Admin, Support, Domain Settings, and AD Explorer. A search bar for AD objects is also present.

The main area has a "Connected Domain: adsp.local.com [Change]" message. On the left, there's a "Dashboard View" section with a "Domain Name : adap.internal.com" header and a "Vital Help Desk Reports" section showing password expiration details. Below it are two bar charts: "User Reports" and "System Reports".

The "User Reports" chart shows the following data:

Category	Value
No. Of Users	2025
Inactive Users	2014
Disabled Users	119
Locked Out Users	0
Password Expired Users	189

The "System Reports" chart shows the following data:

Category	Value
No. Of Computers	60
No. Of Workstations	59
Disabled Computers	3
Domain Controllers	1

To the right, there's a sidebar titled "Inside ADManager Plus" with sections for "AD Management", "AD Reports", and "Helpdesk Delegation", each listing various management tools.

Figure 3.0 Screenshot showing ADManager Plus dashboard

ManageEngine ADManager Plus can be used to automate the report generation process. This lowers the time that would be wasted on manually navigating the Active Directory program, thereby making Active Directory more convenient. Some of the key features of ADManager Plus includes:

- Active Directory Management: This feature simplifies Active Directory management by enabling bulk creation and modification of accounts, delegation, and rep.
- AD Bulk User Management: This feature enables network admins to use CSV files and modify user attributes, reset passwords, move users, and user objects all in bulk.
- Active Directory Bulk User creation: Create and deploy users in bulk with all attributes including Exchange mailbox and terminal services and assign them to groups using CSV import.
- Active Directory Bulk User modification: Enables network admins to reset passwords, unlock users, move users, delete/enable/disable users, add and remove from groups and modify attributes including exchange and terminal services in bulk.

- Inactive/Disabled User Account Management: Enables network admins to clean up AD by generating a list of inactive or disabled accounts that can then be removed or deleted.
- Active Directory Password Management: Reset multiple users' account passwords, configure password settings, and enable/disable users whose passwords expire.
- Mobile Active Directory User Management: Reset passwords, enable, disable, unlock, and delete user accounts from your mobile iOS or Android device.
- Active Directory Computer Management: Create computers, enable, disable, and move computers in bulk and change their general attributes and group memberships in bulk.

ManageEngine ADManager Plus is available for download on a [30-day free trial](#). It is licensed on an annual subscription based on the number of domains it would manage. We recommend this product to anyone looking to make Active Directory Management more convenient as well as those who want to benefit from a high-quality report function.

4. ManageEngine ADAudit Plus: [ADAudit Plus](#) by ManageEngine is an AD auditing tool that allows network admins to audit active directories, login and logoff records, file, and Windows server data, and generate real-time user activity reports. Key AD auditing features include:

- Active Directory auditing
- Windows file server auditing
- NAS device file auditing
- Windows server auditing
- Workstation auditing
- Azure AD auditing

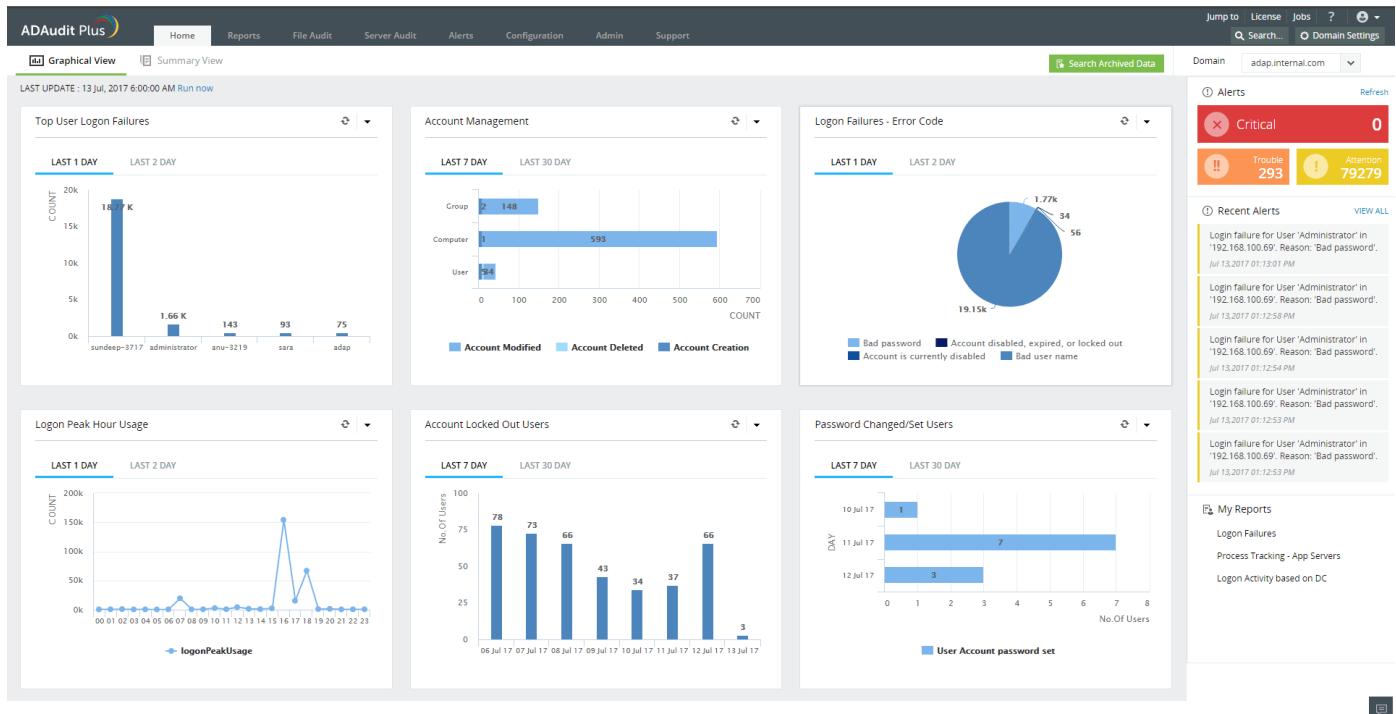


Figure 4.0 Screenshot showing ADAudit Plus dashboard

With this tool, you can keep track of which employees did what, when they did it, and who did it on Windows and File servers. You can get reports on domain controllers and file servers and export the reports to CSV, PDF, XLSX, and HTML formats. Network admins will be able to block or prevent legitimate users from abusing their access privileges. One of the key benefits of this solution is its inherent support for industry-specific regulatory compliance. It is bundled with pre-configured standards compliance reports, which follow the SOX, HIPAA, GLBA, PCI-DSS, and FISMA standards. So, you won't need to customize the system or set up your own reports in order to demonstrate compliance.

ADAudit Plus is available in three editions: Free, Standard, and Professional. A [30-day free trial](#) and an [online demo](#) which includes all features of Professional Edition are all available. Overall, ADAudit Plus' great dashboard and analytics makes it a powerful tool to gain insights and visibility into your AD environment.

5. Quest Recovery Manager for Active Directory: Human error, hardware, and software crashes do occur. AD objects can often be mistakenly modified or even deleted; and faulty scripts can overwrite attributes. This can result in a corrupt Active Directory or Group Policy data, unplanned system downtime.

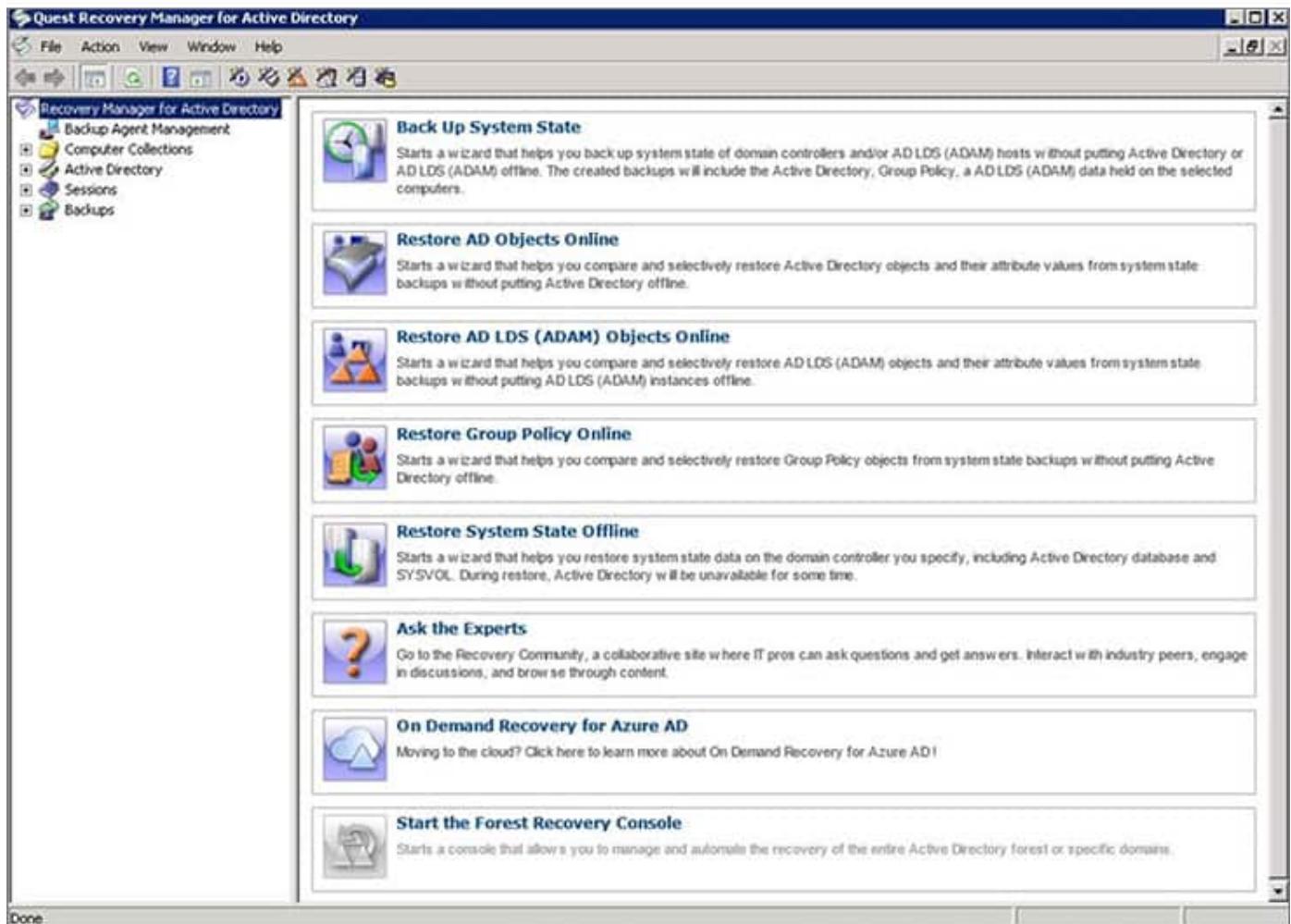


Figure 5.0 Screenshot showing Quest Recovery Manager for Active Directory interface

[Recovery for Active Directory](#) is a third-party AD tool that enables network admins to pinpoint changes to their AD environment at the object and attribute level, and quickly recover entire sections of the directory (both on-premise AD and Azure AD), selected objects, or individual attributes without taking the AD controller offline. In reality, when an object is lost in Active Directory you have to restart the Domain Controller to recover it. Recovery Manager for Active Directory eliminates this inconvenience by allowing you to recover objects without going offline.

You can restore objects such as users, computers, attributes, configurations, sites, subnets group policy objects, and organizational units. Some of the key features include:

- Online restore—Restore directory objects without taking the domain controller offline
- Comprehensive recovery options—Restore any object in AD, including users, groups, computers, organizational units (OUs), sites, subnets, and Group Policy Objects (GPOs)
- Attribute-level restore—Restore only the required attributes without affecting other attributes
- Schedule of AD—Schedule backups and centrally manage system state backups for domain controllers

The main issue with Recovery Manager for Active Directory is that it comes at a relatively high price. It is therefore most suitable for organizations running multiple AD domain controllers across multiple locations. A [free 30-day trial](#) is available.

Active Directory Security Groups FAQs

Why is Windows group policy important in Active Directory from an application security perspective?

Group policy lets you centralize account administration, which means fewer people are involved in controlling security. You can impose global corporate security policies instantly for all user accounts by grouping users. So, standardizing user account settings is quicker with a group policy.

How do I find out if an Active Directory security group is mail enabled?

Only security groups with Universal scope can be mail enabled. You can see whether a group is mail enabled by looking at the group's properties. Right-click on the group and select Properties from the context menu. Open the General tab and if the Email address has a value in it, the group is mail-enabled.

How do I change an Active Directory security group owner?

You can have multiple owners for an Azure Active Directory security group so if you want to replace an owner, you just need to add a new owner and then remove the previous owner. The account that you want to make an owner must already be a member of the group.

1. Log into the Azure Portal with the Administrator account and then open Active Directory.
2. Select **Groups** and then click on the group that you want to change the owner for.
3. In the menu list to the left of the group overview, click on **Owners**.
4. Click on **Add owners**, which will open an overlay panel.
5. In the Add Owners panel, search for and then select the user account that you want to promote.
Click on the **Select** button.
6. Refresh the main group page.
7. Click on **Owners** again. In the Owners screen, click on the owner that you want to remove. Click on the **Remove** button at the top of the screen.
8. Confirm the removal by clicking **Yes** in the popup dialog box.

What security group can only read from Active Directory?

There is a pre-created user group that only allows the members to read Active Directory and not make any changes. This is the **Windows Admin Center Readers** group. You just need to add users to this group.



How to set folder security permissions in Active Directory

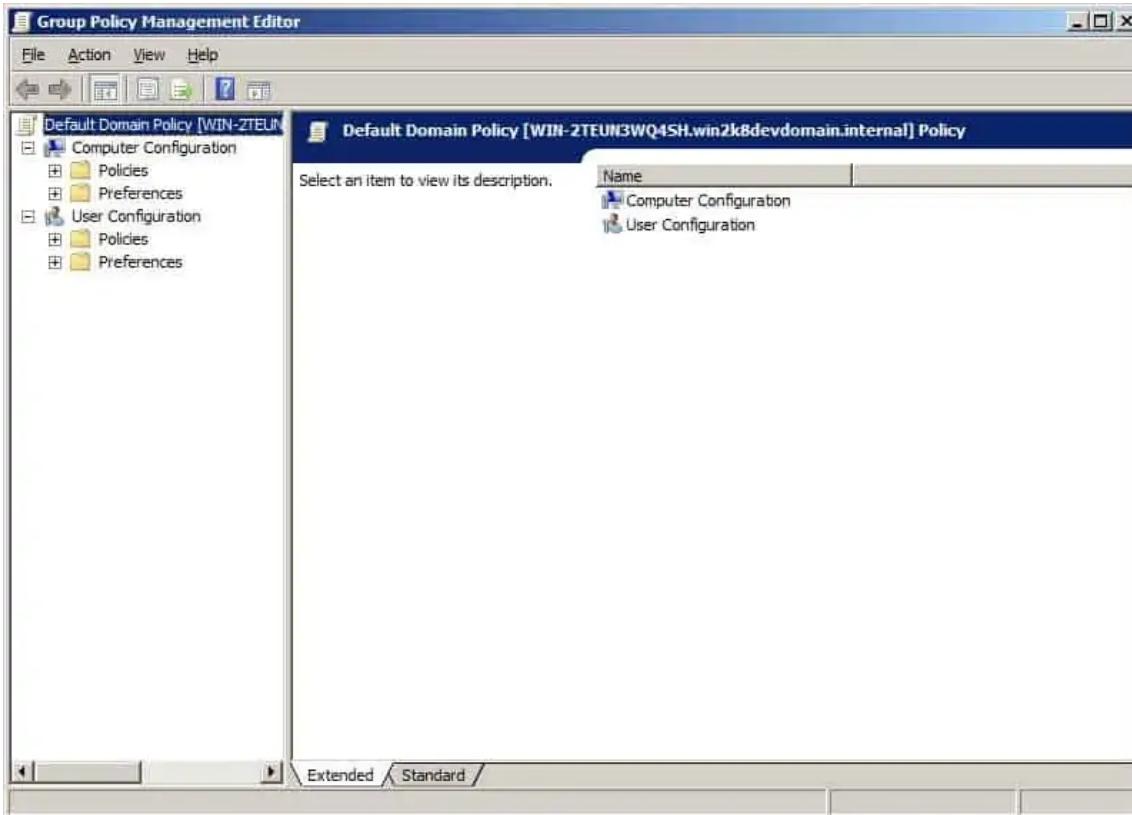
The process of setting folder permissions is simple and you can choose to assign folder access to users and groups. In this section, we're going to look at how you can assign permissions from within Active Directory through the Group Policy Management Console (GPMC).

Creating a Group Policy through the Group Policy Management Console

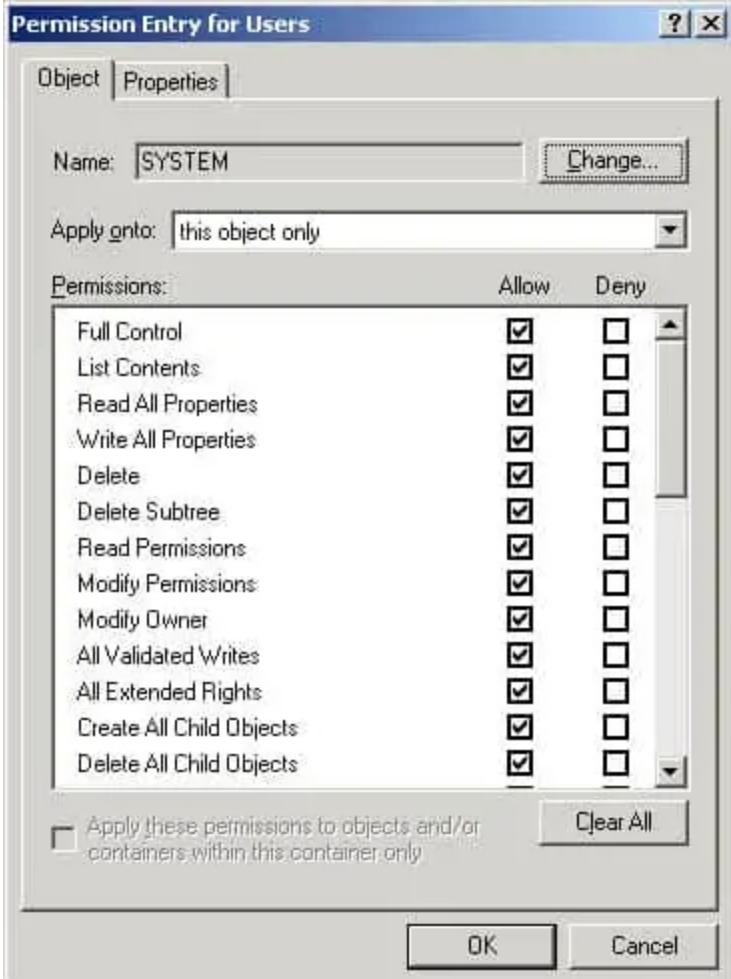
The GPMC provides group policy settings that you can use to configure security permission. One of the simplest ways you can use the program is to create a group policy object. A group policy object is a group of settings that you create with the Group Policy Object Editor that can restrict the access of users to particular files.

To create a new group policy object follow the instructions below:

1. Click Start > Administrative Tools > Group Policy Management. The Group Policy Management Console will display.
2. Right-click on the Group Policy Objects icon and select New. The New GPO window will display.
3. Enter a Name and leave the Source Starter GPO option set as (none).
4. Right-click on the GPO you just created and select Edit GPO. The Group Policy Management Editor window will display.



5. Go to Computer Configuration > Policies > Windows Settings > Security Settings and right-click File System > Add File. The 'Add a file or folder' dialog box will display.
6. Locate the folder or file you want to assign permissions to and click on it. Now press OK.
7. Once the Database Security window comes up, click the Advanced button to display the Advanced Security Settings window.
8. In the Permissions tab, you can assign permission for a new or existing user. To create a new user click Add. If you want to select an existing user, select the user and press Edit.
9. Once the Permission Entry box opens you can view a list of permissions that you can choose to Allow or Deny, as well as determine where those permissions will Apply. Click on the Apply to drop-down menu to choose where you want to apply the permissions.



10. In the Permissions list view, check the permissions that you want to assign to your object. Now press OK.
11. Once you return to the Advanced Security window, go to the Auditing tab. Here you can choose to audit changes to the folder and permissions. You can also go to the Owner tab to configure ownership settings.
12. Once you've entered your settings click OK. Once the Advanced Security window closes click OK again to close the Database Security window.
13. When the Add Object window comes up, you have a number of options: The Configure this file or folder section comes with two sub-options;
 - Option A) Propagate inheritable permissions to all subfolders and files – The first sub-option means that all subfolders will inherit permissions from the parent folder, but if there's a conflict then subfolder permissions will take precedence.
 - Option B) Replace existing permissions on all subfolders and files with inheritable permissions. -The second sub-option means that all subfolder settings will be overwritten by the parent's settings. Alternatively, you can select the Do not allow permissions on this file or folder to be replaced option and create an entry for the specific folder you don't want to inherit permissions. If you select the first option, click OK to close the window.
14. Close the Group Policy Management Editor window and right-click on the domain you want to apply to GPO to and click Link an Existing GPO.
15. Once the Select GPO window displays select the name of the GPO you just created from the list and press OK.
16. Now go to the Linked Group Policy Objects tab and right-click on Assigning Folder Permissions > Enforced. Now press OK to finish.



What is a Service Account?

A service account is a user account that is created explicitly to run a particular service or application on the Windows operating system. If you create service accounts when installing applications that request them, they usually grant the appropriate rights and security permissions when the accounts are created. This is done following the principle of least privilege, which grants users only the minimum rights and permissions they require.

For example, if a service account is created for backup service it does not require rights to change systems settings. A service account that is created to run the SQL Server service does not require access to execute applications. Following the principle of least privilege, a user account with just the right amount of access is created as a service account. You may often be tempted to use an administrator account for a service account since usually they already have the necessary rights and permissions. But don't fall for it. The advantage of the service account is that if the user account used for the service was to become compromised, the damage that could be done using that service account is minimized.

To understand a bit better why a service account is required, let's look at what happens when a service account is not used. When you install applications such as SQL Server, Internet Information Services (IIS), or SharePoint Services on Windows server OS like Windows Server 2012 R2, it is not uncommon for the application to ask for a username and password that will be used to run it. In order to get the application to work, a lot of administrators will simply enter a user account that has domain administrator access. There are a number of problems with this approach.

Firstly, If you use the same user account for a different number of applications, and the user account fails due to one reason or the other, all the applications using that service account would also be affected. Secondly, if the account becomes compromised, this service account could be used to gain access to resources on the network. The more access the service account has the more potential damage that it could do. Thirdly, the service account could prevent applications and services using it from running by simply changing the password of the account.

When the password for a service account is changed, the password must be updated in all locations that use the service account. Otherwise, the old password will still be used and this will prevent the application from running. If all of your essential services are using the same service account and the password is changed, this will cause all the services relying on that service account to stop working, thereby resulting in a denial of service. Although service account passwords are usually configured not to expire; however, the implication is that when you have an account password that doesn't expire, the password becomes much more vulnerable over time.

Managed Service Accounts

After considering all those challenges, Microsoft introduced Managed Service Accounts (MSA) with Windows Server 2008 R2 to automate the management of service accounts. Using managed service accounts means that the password cannot be locked out or used for interactive login. Instead, the service account will be automatically changed periodically without any intervention from the system administrator. The MSA is bound to one computer and thus cannot be shared among multiple computers, or a computer that it was not designed to work with. This provides additional security. The MSA can be categorized into the following groups:

- **Standalone Managed Service Account (sMSA):** sMSA is a managed domain account that provides automatic password management, simplified Service Principal Name (SPN) management, and the ability to delegate it to other administrators. The sMSA was introduced in Windows Server 2008 R2 to automatically manage (change) passwords of service accounts. With sMSA, system admins can mitigate the risk of system accounts running system services being compromised. However, one major issue with sMSA is that the usage of such service accounts is restricted to only one computer. This means that sMSA cannot work with cluster or Network Load Balancing services, which operate simultaneously on multiple servers or server farms and use the same account and password.
- **Group Managed Service Account (gMSA):** To fix issues associated with the sMSA, Microsoft introduced the Group Managed Service Accounts (gMSA) to Windows Server 2012. gMSA provides the same functionality within the domain but also extends that functionality over multiple servers. When a gMSA is used as service principals, the Windows operating system manages the password for the account instead of relying on the administrator to manage the password.

How to Create Service Account in PowerShell

Windows PowerShell is a command-line shell and scripting language built on the .NET Framework to enable system administrators to automate task and configuration management on Windows OS and applications that run on the Windows Server environment. In PowerShell, administrative tasks are generally performed by cmdlets (pronounced command-lets), which are specialized .NET classes that implement specific functions.

In Windows Server 2012, the PowerShell cmdlets default to managing the group MSAs rather than the original standalone MSAs. To create a group Managed Service Accounts (gMSA), follow the steps given below:

Step 1: Create key distribution services (KDS) Root Key.

This is used by the KDS service on the domain controller (DC) to generate passwords. To create the root key, open the PowerShell terminal from the Active Directory PowerShell module and run the following cmdlet:

```
Add-KDSRootKey -EffectiveTime ((Get-Date).AddHours(-8))
```

The 8 hours specified above imply that the Active Directory distribution service replication has within that time frame to replicate the changes to other domain controllers. You can use the following code if you're in a test environment:

```
add-kdsrootkey -EffectiveImmediately
```

You confirm if the key was successfully created by running the following PowerShell command:

```
Get-KdsRootKey
```

Step 2: Create and configure gMSA.

To do this, open the PowerShell terminal and type the following commands:

```
New-ADServiceAccount -Name gserviceaccount1 -DNSHostname DC1.comptech.com -  
PrincipalsAllowedToRetrieveManagedPassword "gserviceaccount1Group"
```

From the above command,

- The gserviceaccount1 represents the name of the gMSA account to be created
- The DC1.comptech.com is the DNS server name
- The gserviceaccount1Group is the Active Directory group which includes all systems that have to be used. This group should be created before in the Groups.

To confirm that the account has been created, go to Server Manager >> Tools >> Active Directory Users and Computers >> Managed Service Accounts.

Step 3: Install the MSA on a host computer in the domain, and make the MSA available for use by services on the host computer.

To install gMSA on a computer, open PowerShell terminal and type in the following commands:

```
Install-ADServiceAccount -Identity gserviceaccount1
```

To confirm that the installation of the gMSA was successful, run the following command:

```
Test-ADServiceAccount gserviceaccount1
```

If the installation was successful, the result should return “True” after running the command as shown in the screenshot below.

Step 4: Configure a service to use the account as its logon identity.

To do this, follow the steps below:

1. Open Server Manager.
2. Click Tools >> Services, to open the Services console
3. Double-click the service to open the services Properties dialog box
4. Click the Log On tab
5. Select “This Account”, and then click Browse
6. Enter the name of the MSA on the text box, and then click OK to save changes
7. On the Log On tab, confirm that the MSA name ends with a dollar (\$) sign
8. When it states that the new logon name will not take effect until you stop and restart the service, click OK.

The account will be given the “Log On as a Service” and the password will be retrieved automatically. If you move a service to another computer and you want to use the same MSA on the target system, you must first use the Uninstall-ADServiceAccount cmdlet to remove the MSA from the current computer and then use the Install-ADServiceAccount cmdlet on the new computer.

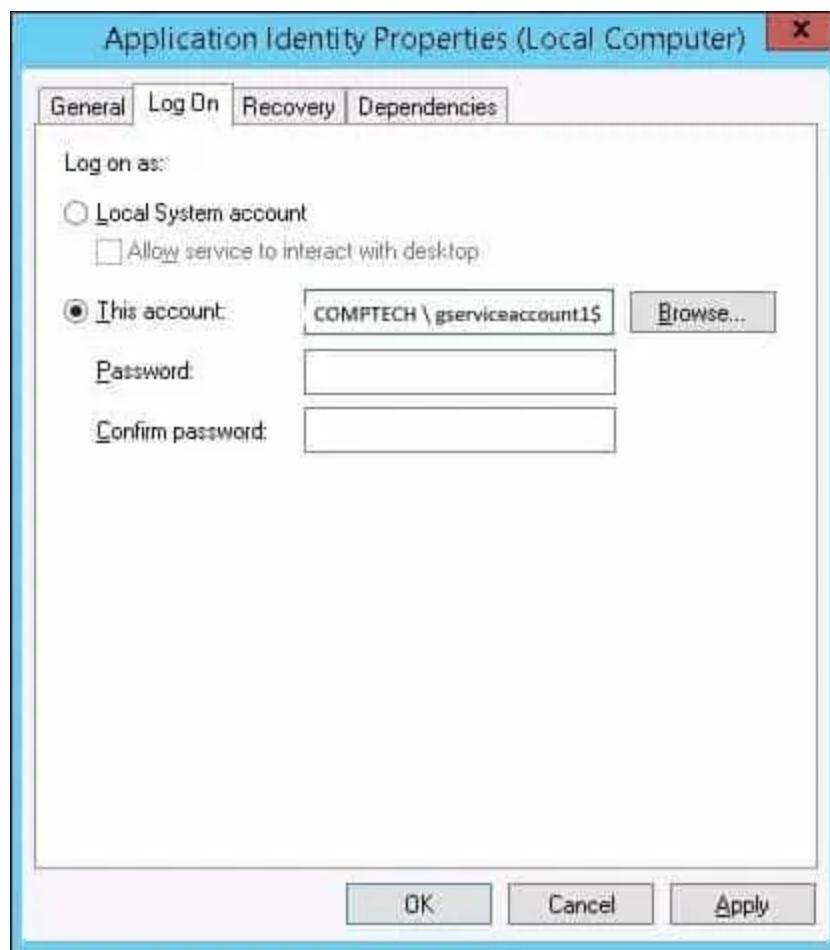


Figure 1.0 Screenshot showing Application Identity Properties settings box



How to...

Backup Active Directory

comparitech

Do you need to back up the active directory?

Active Directory is one of the most important components in any Windows network. Having no backup strategy whatsoever could put the entire organization at risk. Its best practice is to have multiple active directory domain controllers with fail-over functionalities so that when one fails, you would still be able to recover even without a backup. However, having multiple domain controllers is not enough justification to not do a backup. You should still be doing a backup of the active directory whether you have multiple domain controllers or not. Multiple domain controllers can fail at once, accidental or deliberate deletion of all the accounts or critical organizational units (OU) can occur, entire database corruption can occur, viruses, and ransomware or some other disaster could wipe out all domain controllers. In such a situation, you would need to restore it from a backup. This is why you need to backup.

You probably don't need to back up every single domain controller, to get a good backup of the AD. You only really should have to back up one of the domain controllers. If your domain controller crashes, your network and by extension, business activities come to a halt. Although active directory services are designed with high redundancy (if you deployed several DCs in your network). It's therefore important to develop and implement a clear active directory backup policy. If you have multiple DCs running, you need to back up at least one of them. The ideal DC to backup should be the one running the Flexible Single Master Operation (FSMO) role. With a good backup and recovery strategy implementation, your organization can easily recover after your domain controllers crash.

If the Active Directory Domain Controller (AD DC) becomes unavailable for whatever reason, then users cannot log in and systems cannot function properly, which can cause disruption to business activities. That's why backing up your Active Directory is important. In this article, we will show you how to backup an Active Directory domain controller running on Windows Server 2019. Before we begin we will take a look at a concept known as System State backup and how it affects Active Directory data.

System State backup

Microsoft Windows Server offers the possibility to perform a 'Full' backup or a 'System State' backup. A Full backup makes a copy of the system drives of a physical or a virtual machine, including applications, operating systems, and even the System State. This backup can be used for bare metal recovery—this allows you to easily reinstall the operating system and use the backup to recover.

System State backup on the other hand creates a backup file for critical system-related components. This backup file can be used to recover critical system components in case of a crash. Active Directory is backed up as part of the System State on a domain controller whenever you perform a backup using [Windows Server Backup](#), Wbadmin.exe, or PowerShell. For the purpose of this guide, we will be using System State backup because it allows us to backup only the components needed to restore Active Directory. However note that Microsoft does not support restoring a System State backup from one server to another server of a different model, or hardware configuration. The System State backup is best suited for recovering Active Directory only on the same server.

As described later in this guide, Windows Server Backup must be installed through features in Server Manager before you can use it to back up or recover your server. The type of backup you select for your domain controllers will depend on the frequency of changes to Active Directory and the data or applications that might be installed on the domain controller. The bare minimum you need to back up to protect essential Active Directory data on a domain controller is the System State. The System State includes the following list plus some additional items depending on the roles that are installed:

- Domain controller: Active Directory DC database files (NTDS.DIT), boot files & system protected files, COM+ class registration database, registry, system volume (SYSVOL)
- Domain member: Boot files, COM+ class registration database, registry
- A machine running cluster services: Additionally backs up cluster server metadata
- A machine running certificate services: Additionally backs up certificate data

In addition, System State backups will back up Active Directory-integrated [DNS](#) zones but will not back up file-based DNS zones. File-based DNS zones must be backed up as part of a volume-level backup, such as a critical volume backup or full server backup. All the above backup types can be run manually on-demand, or they can be scheduled using Windows Server Backup. You can use either Windows Server backup or Wbadmin.exe to perform a System State backup of a domain controller to back up Active Directory. Microsoft recommends using either a dedicated internal disk or an external removable disk such as a USB hard disk to perform the backups.

Backup operators do not have the privileges required to schedule backups. You must have administrative rights to be able to schedule a System State backup or restore. A System State backup is particularly important for disaster recovery purposes as it eliminates the need to reconfigure Windows back to its original state before the system failure occurred. It is important that you always have a recent backup of your System State. They may require you to perform regular System State backups to increase your level of protection. We recommended that you perform System State backups before and after any major change is made to your server.

Before going ahead with the backup process, you need to take note of the following initial steps:

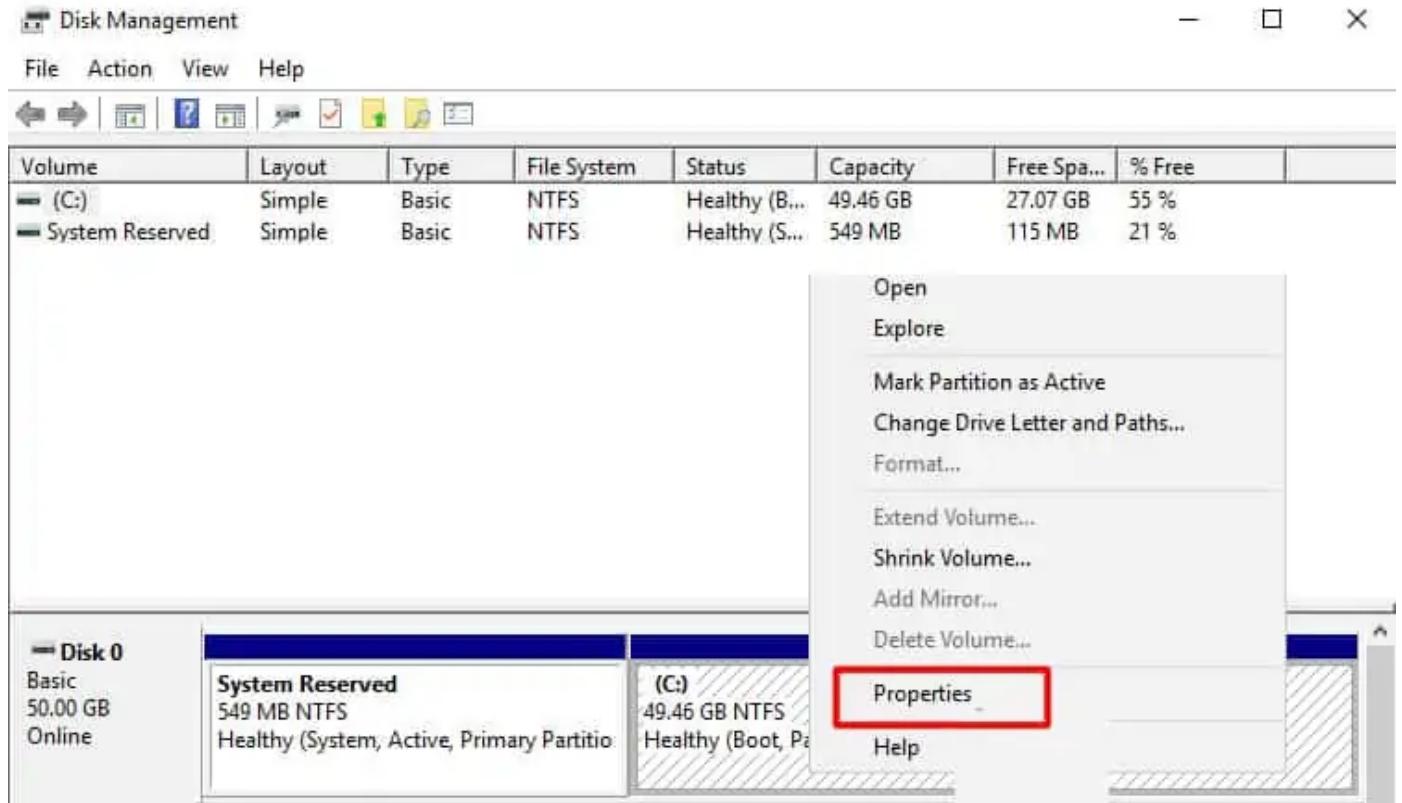
1. It is important that you have the necessary amount of storage space to accommodate the backup you are about to perform.
2. If you're going to be backing up while the applications that produce the data are still running (which is usually the case), you need to configure the Volume Shadow Copy Service, also known as Volume Snapshot Service (VSS) on the drive for the backup to be successful. This service helps to create backup copies or snapshots of computer files or volumes, even when they are in use.
3. You need to install the Windows Server Backup feature if you haven't done this yet. Windows Server 2019 just like previous editions, comes with the Windows Server Backup feature that helps to perform Active Directory database backups and restores. Now we will go through the above steps in detail.

Configure the Volume Shadow Copy Service (VSS)

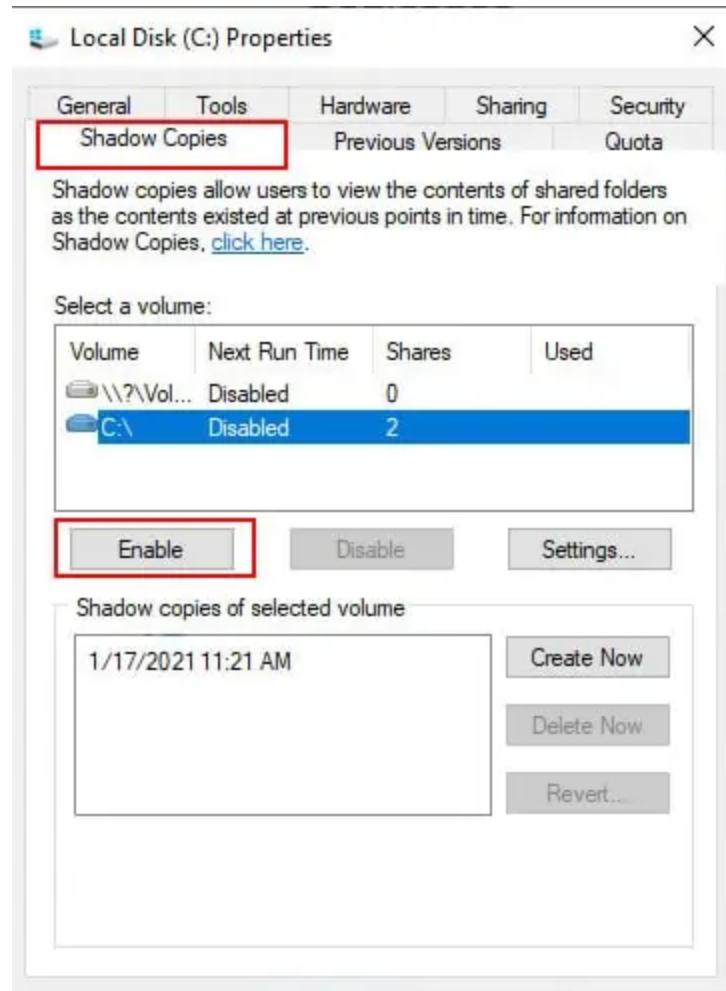
It is important to ensure that the AD database is backed up in a way that preserves database consistency. One way to preserve consistency is to back up the AD database when the server is in a powered-off state. However, backing up the Active Directory server in a powered-off state may not be a good idea if the server is operating in 24/7 mode.

For this reason, Microsoft recommends the use of Volume Shadow Copy Service (VSS) to back up a server running Active Directory. VSS is a technology included in Microsoft Windows that can create backup copies or snapshots of computer files or volumes, even when they are in use. VSS writers create a snapshot that freezes the System State until the backup is complete to prevent modifying active files used by Active Directory during a backup process. In this way, it is possible to back up a running server without affecting its performance. For this guide, we are going to show you how to change the Shadow Copy size limit configuration on the volume where we are going to store the AD database.

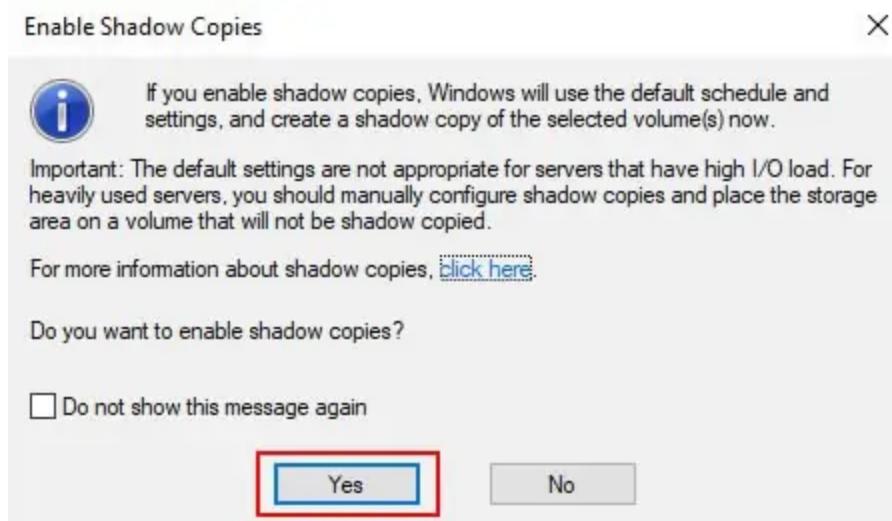
1. Press a combination of Win+X on your keyboard to open the Disk Manager. Select the partition where the server is installed, then right-click on it and click on **Properties**.



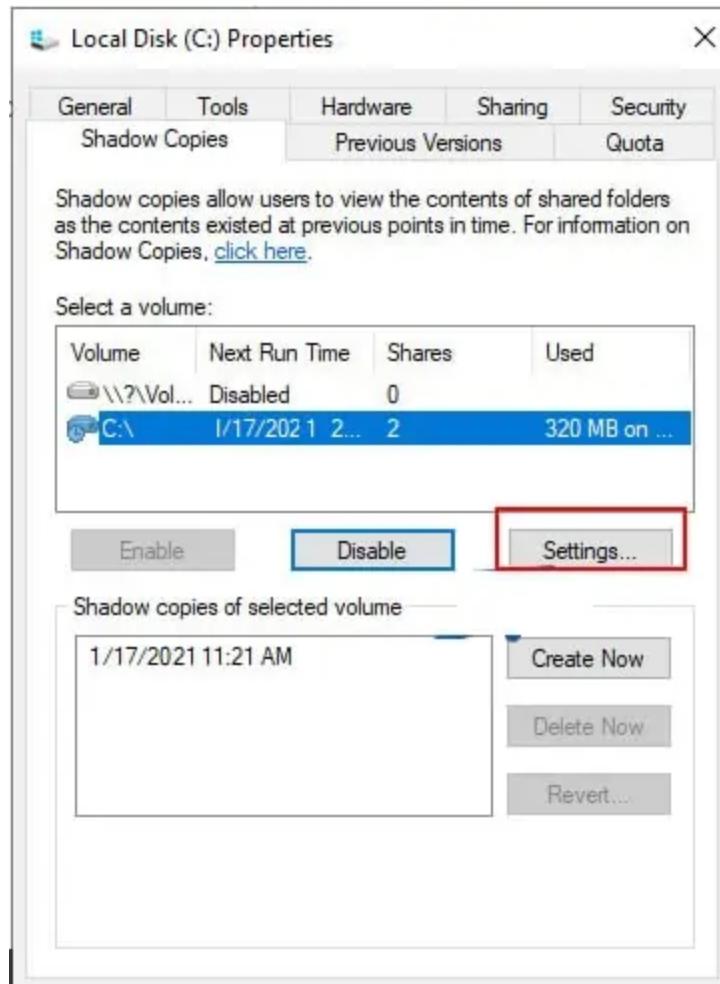
2. Go to the **Shadow Copies** tab and then click on **Enable** as shown on the image below.



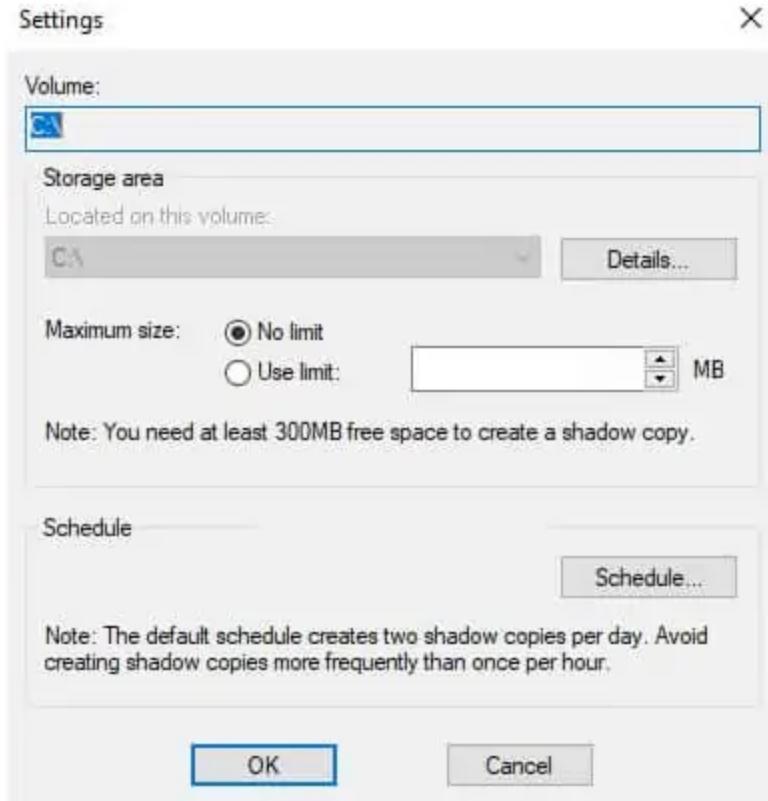
3. In the next window, click **Yes** to confirm that you want to enable shadow copies as shown below.



4. After confirmation, you'll see a restore point created in the selected partition. Click on **Settings** to continue.



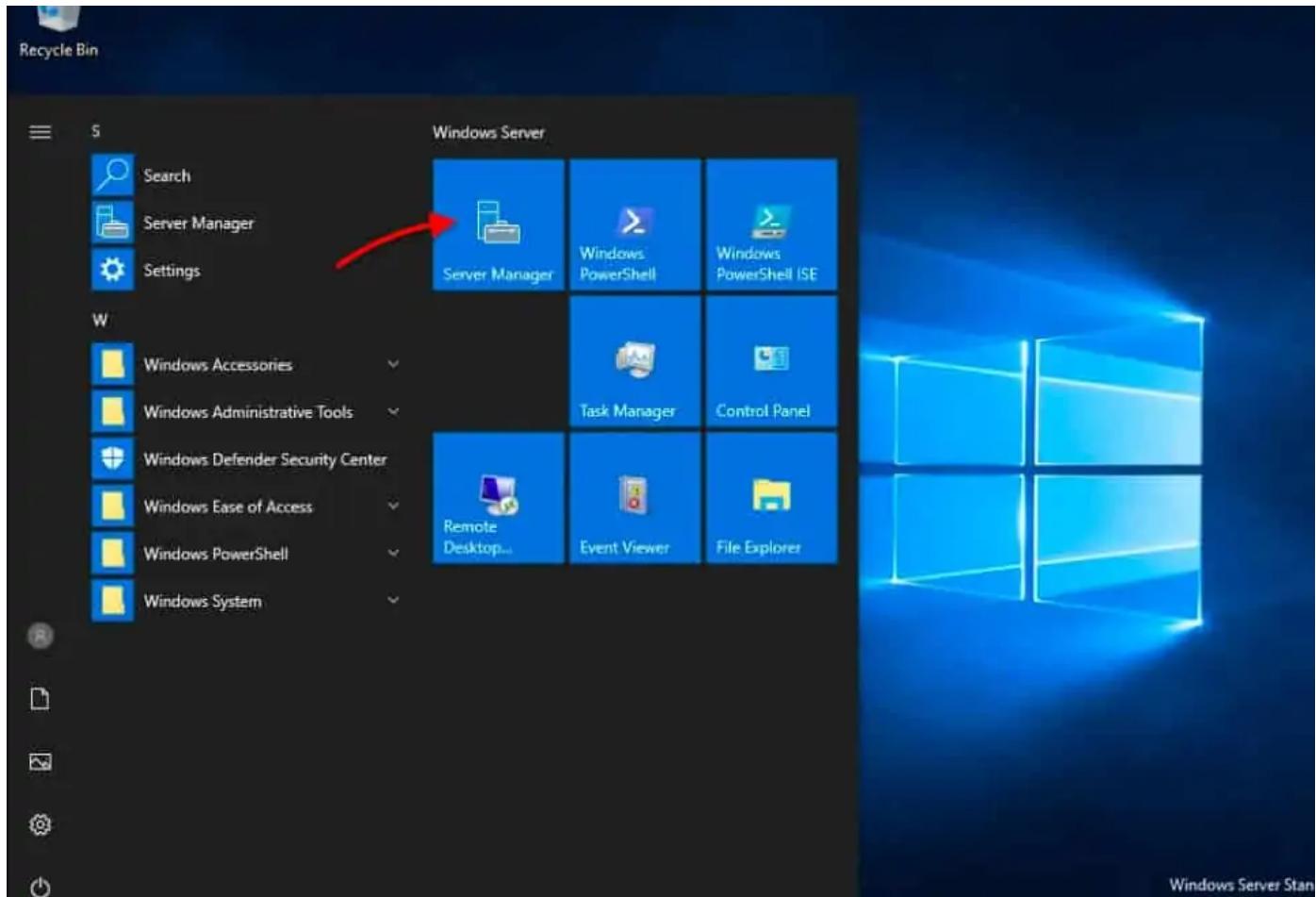
5. In the **Settings** screen shown below, under **Maximum size**, select **No limit**. Once completed click the **OK** button, and that does it for this section—configure the Volume Shadow Copy Service (VSS).



Install the Windows Server backup feature

Windows Server Backup is a utility provided by Microsoft with Windows Server 2008 and later editions. It replaced the NTBackup utility which was built into the Windows Server 2003. Windows Server Backup is a feature that is installable in Windows Server 2019 just like in other previous editions. So if you haven't used the backup feature yet, you will likely have to install it first. The way to install this feature is through the Server Manager.

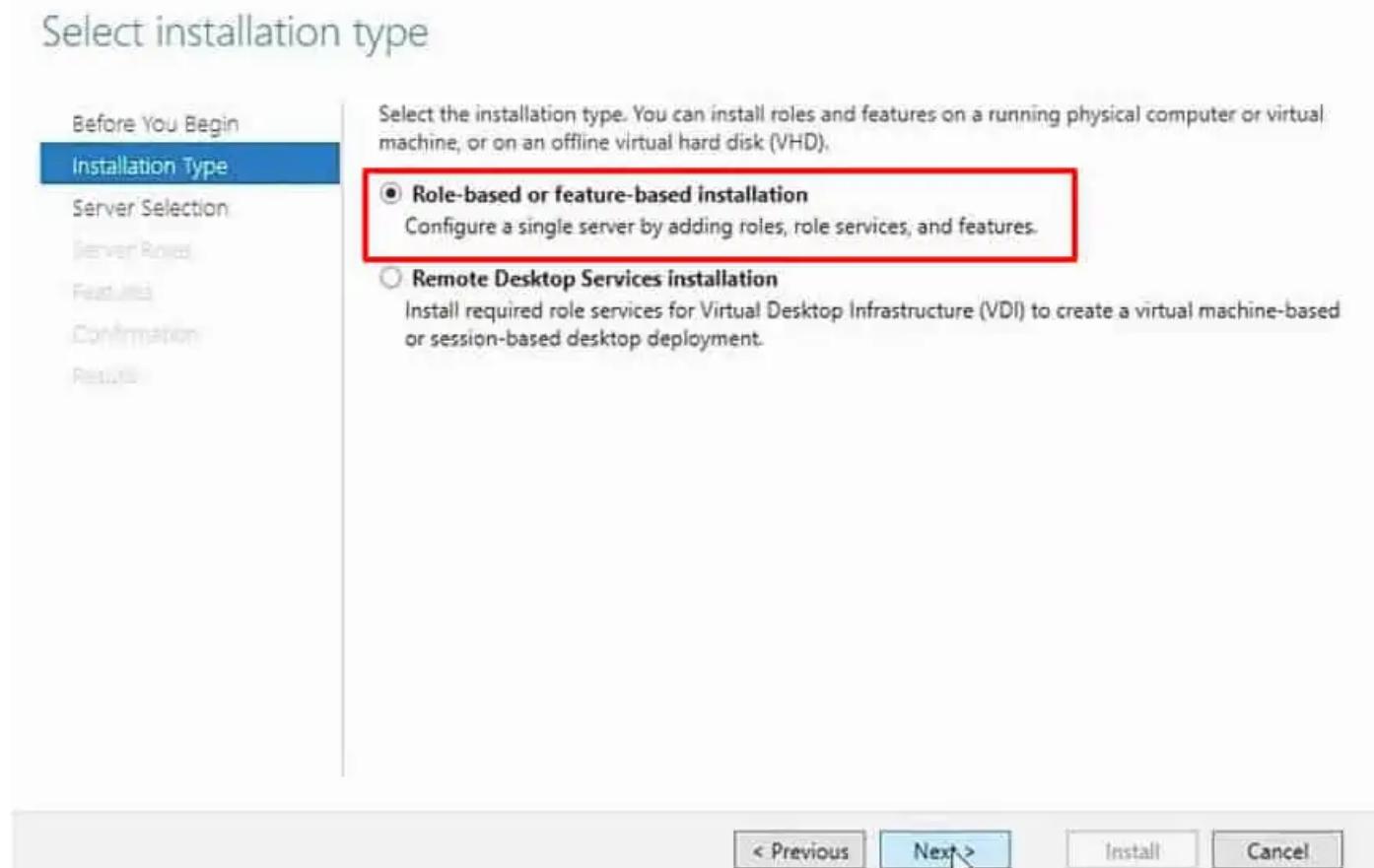
1. Open the Server Manager console as shown in the image below.



2. Go to **Local Server >> Manage tab >>** and click on the **Add Roles and Features** as seen in the image below. This will open the Add Roles and Features Wizard.

A screenshot of the Server Manager interface. The left navigation pane shows 'Dashboard', 'Local Server' (which is selected and highlighted in blue), 'All Servers', 'AD DS', 'DNS', and 'File and Storage Services'. The main content area displays 'PROPERTIES For W52K19-DC01' for the computer 'For W52K19-DC01'. It includes sections for Computer name, Domain, Windows Defender Firewall, Remote management, Remote Desktop, NIC Teaming, Ethernet, Operating system version, and Hardware information. On the right, a 'Manage' ribbon tab is selected, showing options like 'Add Roles and Features' (which is highlighted with a red box and a red arrow), 'Remove Roles and Features', 'Add Servers', 'Create Server Group', and 'Server Manager Properties'. The status bar at the bottom right shows 'Windows Server Standard'.

3, In the **Select installation type** screen, select the **Role-based or feature-based installation** option and click **Next**.



4. In the next screen called **Select destination server**, you will be required to select the server on which you want to install roles and features. Windows will automatically display the server pool. In this case, we are going to select the local server, which is **WD2K19-DC01-mylablocal**.

Select destination server

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Changelog
Results

Select a server or a virtual hard disk on which to install roles and features.

Select a server from the server pool
 Select a virtual hard disk

Server Pool

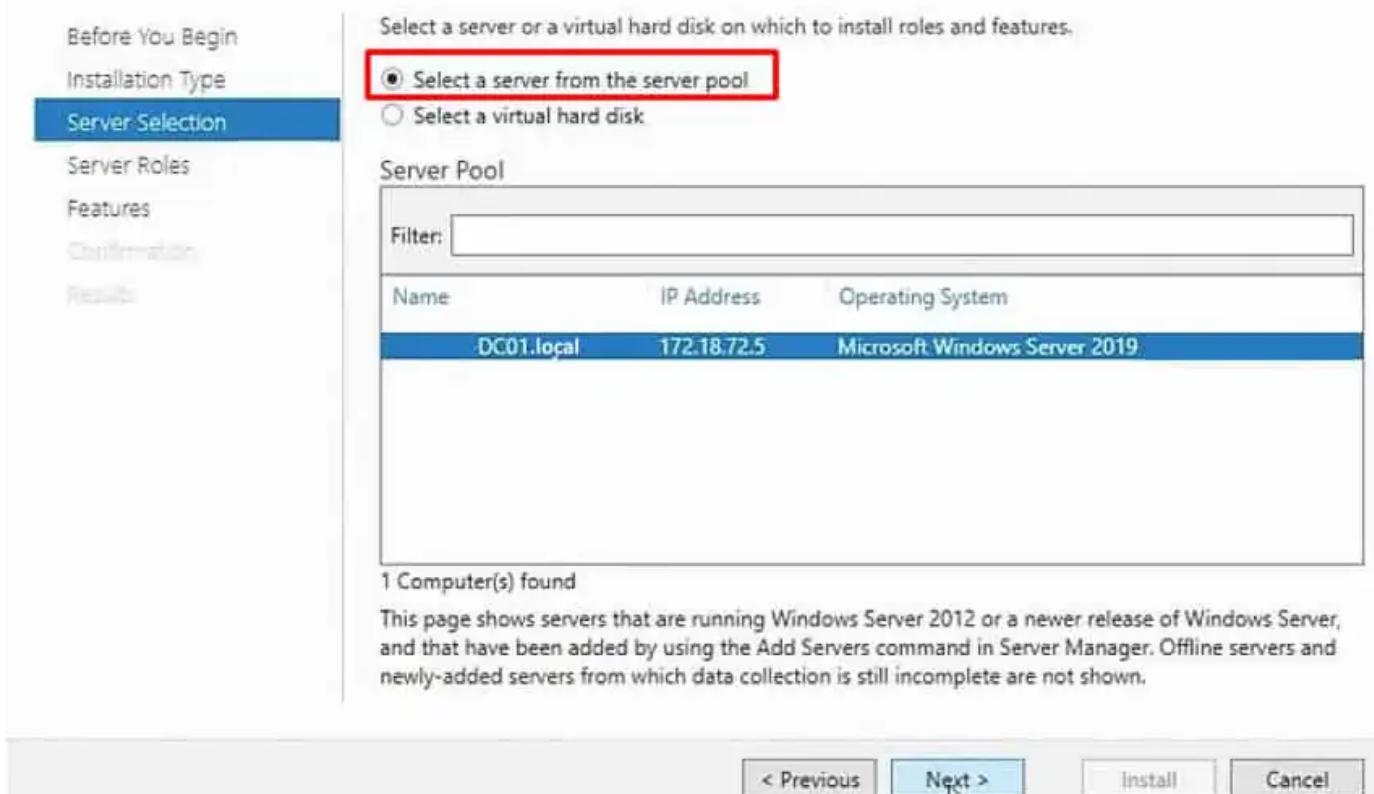
Name	IP Address	Operating System
DC01.local	172.18.72.5	Microsoft Windows Server 2019

Filter:

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

< Previous **Next >** Install Cancel



5. In the **Select server roles** screen, you are required to select the roles to install on the server. Since we are installing a feature, you can ignore this section and continue to the next screen. Click **Next** to continue.

Select server roles

The screenshot shows the 'Select server roles' screen of the Windows Server Setup Wizard. On the left, a vertical navigation bar lists steps: 'Before You Begin', 'Installation Type', 'Server Selection', 'Server Roles' (which is selected and highlighted in blue), 'Features', 'Confirmation', and 'Results'. The main area has a title 'Select one or more roles to install on the selected server.' Below it is a 'Roles' section containing a list of checkboxes. Some checkboxes are checked (e.g., Active Directory Domain Services, DNS Server, File and Storage Services), while others are empty (e.g., Active Directory Certificate Services, Active Directory Federation Services). To the right of the list is a 'Description' column for the selected role, which is 'File and Storage Services'. At the bottom are buttons for '< Previous', 'Next >' (which is highlighted with a red box), 'Install', and 'Cancel'.

Role	Description
<input type="checkbox"/> Active Directory Certificate Services	Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.
<input checked="" type="checkbox"/> Active Directory Domain Services (Installed)	
<input type="checkbox"/> Active Directory Federation Services	
<input type="checkbox"/> Active Directory Lightweight Directory Services	
<input type="checkbox"/> Active Directory Rights Management Services	
<input type="checkbox"/> Device Health Attestation	
<input type="checkbox"/> DHCP Server	
<input checked="" type="checkbox"/> DNS Server (Installed)	
<input type="checkbox"/> Fax Server	
<input checked="" type="checkbox"/> File and Storage Services (2 of 12 installed)	
<input type="checkbox"/> Host Guardian Service	
<input type="checkbox"/> Hyper-V	
<input type="checkbox"/> Network Controller	
<input type="checkbox"/> Network Policy and Access Services	
<input type="checkbox"/> Print and Document Services	
<input type="checkbox"/> Remote Access	
<input type="checkbox"/> Remote Desktop Services	
<input type="checkbox"/> Volume Activation Services	
<input type="checkbox"/> Web Server (IIS)	
<input type="checkbox"/> Windows Deployment Services	

6. In the **Select features** screen below, scroll down to the **Windows Server Backup** feature, and select it as seen in the image below. Click **Next** to continue.

Select features

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select one or more features to install on the selected server.

Features

<input type="checkbox"/> VM Shielding Tools for Fabric Management
<input type="checkbox"/> WebDAV Redirector
<input type="checkbox"/> Windows Biometric Framework
<input checked="" type="checkbox"/> Windows Defender Antivirus (Installed)
<input type="checkbox"/> Windows Identity Foundation 3.5
<input type="checkbox"/> Windows Internal Database
<input checked="" type="checkbox"/> Windows PowerShell (2 of 5 installed)
<input type="checkbox"/> Windows Process Activation Service
<input type="checkbox"/> Windows Search Service
<input checked="" type="checkbox"/> Windows Server Backup
<input type="checkbox"/> Windows Server Migration Tools
<input type="checkbox"/> Windows Standards-Based Storage Management
<input type="checkbox"/> Windows Subsystem for Linux
<input type="checkbox"/> Windows TIFF IFilter
<input type="checkbox"/> WinRM IIS Extension
<input type="checkbox"/> WINS Server
<input type="checkbox"/> Wireless LAN Service
<input checked="" type="checkbox"/> WoW64 Support (Installed)
<input checked="" type="checkbox"/> XPS Viewer (Installed)

Description

Windows Server Backup allows you to back up and recover your operating system, applications and data. You can schedule backups, and protect the entire server or specific volumes.

< Previous

Next >

Install

Cancel

7. In the **Confirm installation selections** screen, make sure that the Windows Server Backup feature is on the screen and click on the **Install** button to begin the installation.

Confirm installation selections

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

To install the following roles, role services, or features on selected server, click Install.

Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Windows Server Backup

Export configuration settings

Specify an alternate source path

< Previous

Next >

Install

Cancel

The Windows Server Backup feature will begin to install on your local server. Once the installation is completed, click the **Close** button to close the console.

Installation progress

The screenshot shows the 'Installation progress' window. On the left, a vertical navigation bar lists steps: 'Before You Begin', 'Installation Type', 'Server Selection', 'Server Roles', 'Features', 'Confirmation', and 'Results'. The 'Results' step is highlighted with a blue background. The main area is titled 'View installation progress' and shows a section for 'Feature installation' with a progress bar indicating completion. A message states 'Installation succeeded on win19test.cloud.local.' Below this, there's a section titled 'Windows Server Backup' which is currently empty. At the bottom, a note says 'You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.' There are also 'Export configuration settings' and 'Close' buttons.

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

View installation progress

i Feature installation

Installation succeeded on win19test.cloud.local.

Windows Server Backup

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

< Previous Next > **Close** Cancel

Backup the Active Directory database

1. Now go to the Server Manager and click on **Tools >> Windows Server Backup**, in order to open it. You can also open this console by running the command **wbadmin.msc** on the Windows Run (Ctrl+R). Once it opens up, you'll be able to see the scheduled and last backup status (unless this is the first time you're doing this.)

The screenshot shows the Windows Server Manager interface for a local server named WS2K19-DC01. The left navigation pane includes options like Dashboard, Local Server (which is selected), All Servers, AD DS, DNS, and File and Storage Services. The main content area has two sections: 'PROPERTIES' and 'EVENTS'. The 'PROPERTIES' section displays basic system information such as computer name, domain, network configuration, and hardware details. The 'EVENTS' section shows a list of 32 total events, with one entry for 'WS2K19-DC01' on 6/21/2019 at 9:42:01 AM. A red box highlights the 'Tools' menu item in the top right, which lists various management tools. Another red box highlights the 'Windows Server Backup' option under the Tools menu.

2. Once the server backup opens, click on **Backup Once** to initiate a manual AD database backup. Although you can also create automatic scheduled backups by clicking Backup schedule, for this guide we are going to create a manual backup.

The screenshot shows the Windows Server Backup application window. The left sidebar shows 'Windows Server Backup (Local)' and 'Local Backup' is selected. The main area is titled 'Local Backup' and contains instructions: 'You can perform a single backup or schedule a regular backup using this application.' It also states 'No backup has been configured for this computer. Use the Backup Schedule Wizard or the Backup Once Wizard to perform a backup.' Below this is a 'Messages' section with a table showing activity from the previous week. The right sidebar is titled 'Actions' and lists options: 'Local Backup', 'Backup Schedule...', 'Backup Once...' (which is highlighted with a red box), 'Recover...', 'Configure Performance Sett...', 'View', and 'Help'. A hand cursor icon points towards the 'Backup Once...' option.

3. Under Backup Options select **Different options** and click on the **Next** button This option is used where there is no scheduled backup.



Backup Options

Backup Options

Select Backup Configurat...

Specify Destination Type

Select Backup Destination

Confirmation

Backup Progress

Create a backup now using:

Scheduled backup options

Choose this option if you have created a scheduled backup and want to use the same settings for this backup.

Different options

Choose this option if you have not created a scheduled backup or to specify a location or items for this backup that are different from the scheduled backup.

To continue, click Next.

< Previous

Next >

Backup

Cancel

4. In the **Select Backup Configuration** screen, you have two options:

- Full Server backs up all server data, applications, and System State
- Custom lets you choose what you want to back up.

Since we just want to back up the active directory, we choose the second option. So select **Custom** and click **Next**.



Select Backup Configuration

Backup Options

Select Backup Configuration...

Select Items for Backup

Specify Destination Type

Select Backup Destination

Confirmation

Backup Progress

What type of configuration do you want to schedule?

Full server (recommended)

I want to back up all my server data, applications and system state.

Backup size: 29.24 GB

Custom

I want to choose custom volumes, files for backup.

< Previous

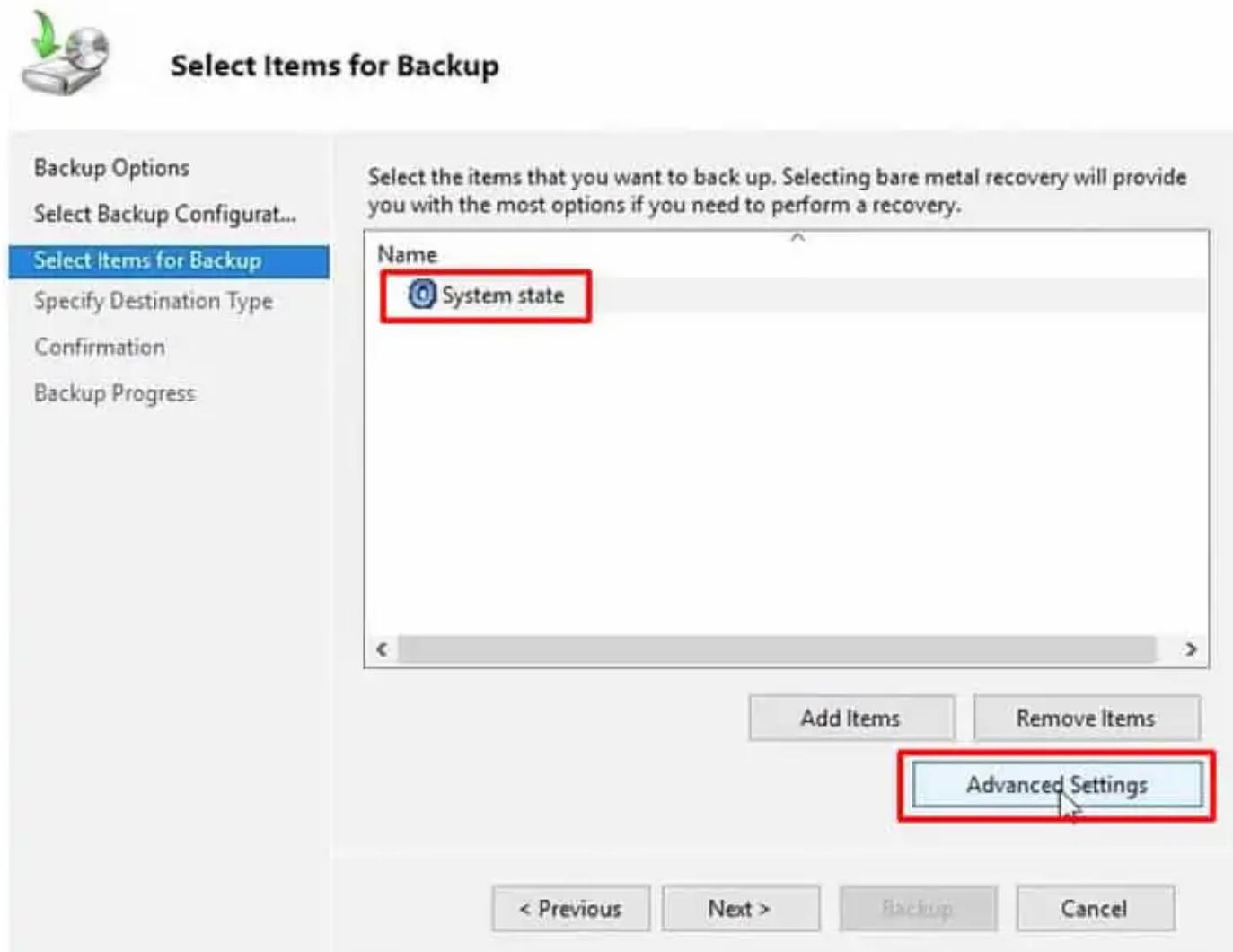
Next >

Backup

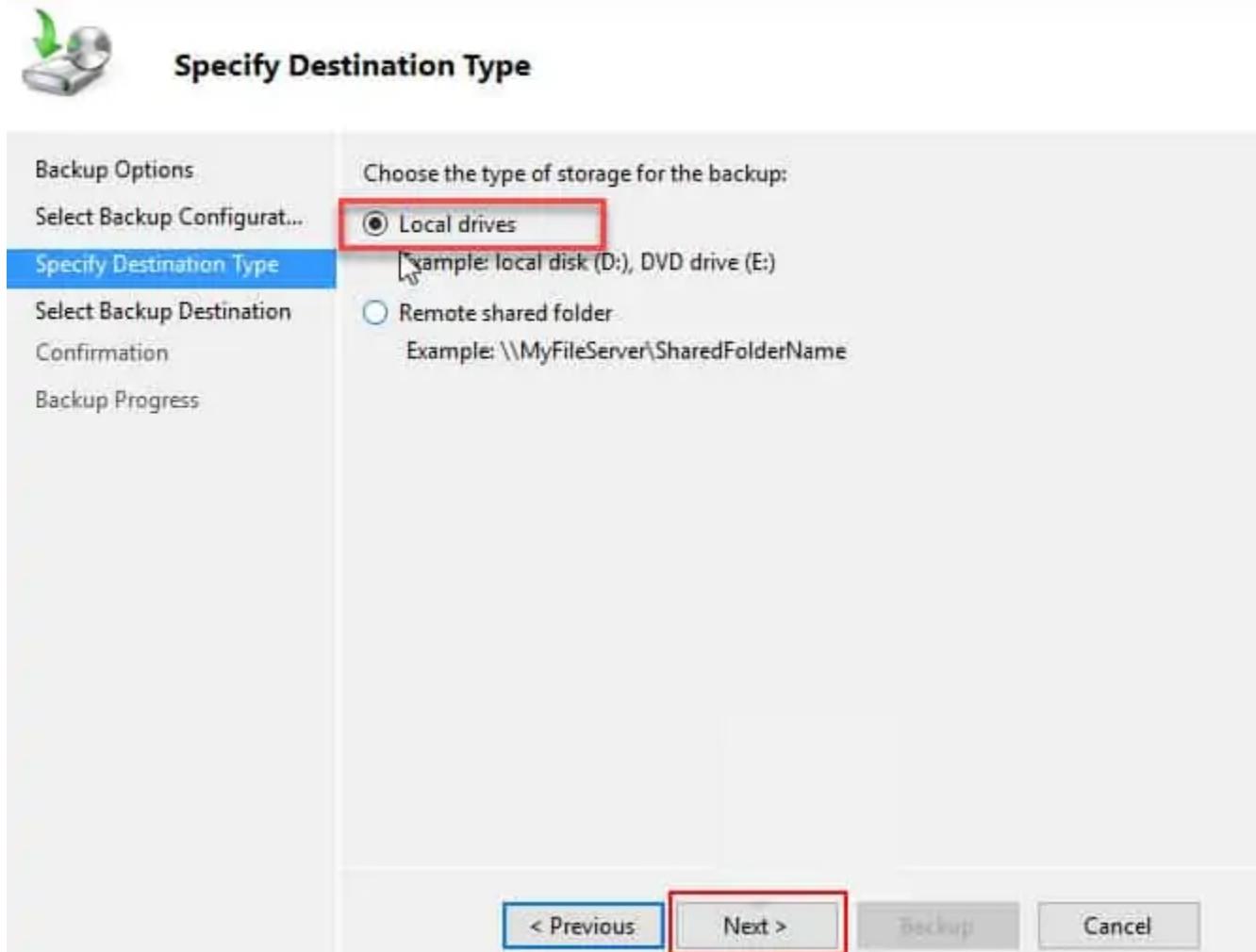
Cancel

5. In the **Select Items for Backup** screen, specify the items that you want to include in the backup. In this backup, we are going to choose the **System State** Backup item. To do this, click on the **Add items** button >> select **System State** option >> and click on the **Ok** button to complete the process.

6. Now we are going to enable the Volume Shadow Copy Service for this backup item. Doing this prevents AD data from being modified while the backup is in progress. To enable VSS, click on **Advanced Settings** >> **VSS Settings** >> Select **VSS Full Backup**, and click **Ok**. The **VSS Full Backup** is the recommended option if it is your first backup, and you are not using any third-party backup tool. This option allows you to create a backup of all the files. It is also the preferred method for incremental backups, as it does not affect the sequence of backup.



7. In the next screen, you would need to specify the backup destination type – **Local drives** or **Remote shared folder**. For the purpose of this demonstration, we are using a local hard drive to store the backup. So choose **Local drives** and click **Next**.



8. In the **Select Backup Destination** screen you can choose the actual partition where you want to store the backup. Once you are done, click **Next** to proceed to the next screen.



Select Backup Destination

Backup Options

Select Backup Configuration...

Select Items for Backup

Specify Destination Type

Select Backup Destination

Confirmation

Backup Progress

Select a volume to store the backup. An external disk attached to this computer is listed as a volume.

Backup destination:

New Volume (E)

Total space in backup destination:

30.00 GB

Free space in backup destination:

21.27 GB

< Previous

Next >

Backup

Cancel

9. The **Confirmation** screen lets you double-check that all backup parameters are correctly configured. Once you are good to go, click the **Backup** button. The backup should take some time depending on the size of the domain controller server. Once the backup is successfully completed, you can close the Backup Wizard.



Confirmation

Backup Options

Select Backup Configurat...

Select Items for Backup

Specify Destination Type

Select Backup Destination

Confirmation

Backup Progress

A backup of the items below will now be created and saved to the specified destination.

File excluded: None

Backup destination: New Volume (E:)

Advanced option: VSS Copy Backup

Backup items

Name
System state

< Previous

Next >

Backup

Cancel

If you closed the Backup Wizard without waiting for the last message status, the backup will continue to run in the background. You can also confirm the status and completion results of the backup from the webadmin console (or Windows Server Backup Feature). The console will display a message with information from this backup (and others).

The best Active Directory tools

Whether you're looking for an automated alerts system, a more convenient user management interface, or reporting, then there is a product available for you.

What should you look for in Active Directory tools?

We reviewed the market for AD management software and analyzed the options based on the following criteria:

- A facility to analyze the permissions structure
- A system to automate user account and group creation
- An audit trail that logs all changes to AD entries
- An assessment feature that helps to tighten security
- An abandoned account identifier
- A free trial period or a money-back guarantee to aid risk-free assessment
- A value for money package that is worth paying for or a free tool that is worth installing

When assessing Microsoft AD management tools that made our 'best of' list, our main considerations were the ease of getting the tools working and how easy it is to use, it's robustness and reliability, the amount of support and regularity of updates the tool received and its overall relative value.

1. SolarWinds Permissions Analyzer for Active Directory (FREE TOOL)

The screenshot shows the SolarWinds Permissions Analyzer for Active Directory interface. The main window title is "SolarWinds Permissions Analyzer for Active Directory". In the top left, there's a "Dashboard" button, followed by "Group or User" and a dropdown menu containing "\\test.local\testUser". Below that is a "File or Folder" section with "NEW!" and a dropdown menu containing "\\mmt-001-win2008r2\TestShare", with a "BROWSE" button next to it. A large orange "Analyze" button is centered above a table. On the left, there are three vertical tabs: "Power Up" (highlighted), "Get Geeky", and "Free Tools". The main table displays file permissions for the specified user and folder. The columns are "Permission name", "NTFS", "Share", and "Total". The rows list various permissions: AppendData, ChangePermissions, CreateDirectories, CreateFiles, Delete, DeleteSubdirectoriesAndFiles, ExecuteFile, and FullControl. Most permissions are marked as "inherited*", except for ExecuteFile which is marked as "+". The "Share" column contains green checkmarks for AppendData, ChangePermissions, CreateDirectories, CreateFiles, Delete, DeleteSubdirectoriesAndFiles, and FullControl, while ExecuteFile has a red X. The "Total" column shows a red X for all permissions except ExecuteFile, which has a green checkmark.

Permission name	NTFS	Share	Total
AppendData	inherited*	✓	✗
ChangePermissions	inherited*	✓	✗
CreateDirectories	inherited*	✓	✗
CreateFiles	inherited*	✓	✗
Delete	inherited*	✓	✗
DeleteSubdirectoriesAndFiles	inherited*	✓	✗
ExecuteFile	+	✓	✓
FullControl	inherited*	✓	✗

First up on this list we have [SolarWinds Permissions Analyzers for Active Directory](#). One of the most common complaints made of the original Active Directory program is that it offers poor permissions management. SolarWinds Permissions Analyzer for Active Directory is an AD management tool that seeks to rectify this by allowing you to view which users in your network have permission to which data.

Key Features

- Free to use
- Provides an overview
- Shows permissions by group or user
- Low processing power requirements
- File permissions

This means that in a live networking environment you will be able to quickly identify which members of your team have access privileges to sensitive data. You can do this by viewing permissions by group or individual user. You can also see why a user has privileges to certain information.

Pros:

- Highly visual and intuitive tool that is great for both small and large Active Directory environments
- Top down view allows you to quickly spot permission issues based on shares, security groups, or individual users
- Lightweight tools – won't bog down important services running on AD
- Great for auditing compliance
- Completely free

Cons:

- While the tool is easy to use, it features an advanced tab that contains a lot of options that can take time to fully explore

As an added bonus, SolarWinds Permissions Analyzer for Active Directory is available for free. This is great because you can start monitoring your network permissions without having to spend a fortune in order to be able to do so. SolarWinds Permissions Analyzer for Active Directory can be [downloaded free](#).

EDITOR'S CHOICE

With SolarWinds Permission Analyzer for Active Directory you get a powerful dashboard that will give you insights on network shares, files and folders that users have access to. You can browse permission at the group or even individual levels. Lots of power for a free Active Directory tool.

Download Free Tool: solarwinds.com/free-tools/permissions-analyzer-for-active-directory

OS: Windows

2. ManageEngine ADManager Plus

ManageEngine **ADManager** plus

Welcome, admin
Sign Out | Change Password | Jump To

Home AD Mgmt AD Reports AD Delegation Workflow Admin Support Domain Settings | AD Explorer

Connected Domain: adsp.local.com [Change]

Dashboard View

A quick snapshot of all essential and top level information of domains.

Domain Name : [adap.internal.com](#) [Edit Domain Details](#)

Vital Help Desk Reports
Essential help desk reports at a glance

Passwords expiring in 7 days : 1 Password expired users : 189

[Change password at next logon](#) [Options](#)

Canned Reports
Overall reports on Active Directory objects [Update Dashboard](#)

User Reports

Category	Value
No. Of Users	2025
Inactive Users	2014
Disabled Users	119
Locked Out Users	0
Password Expired Users	189

System Reports

Category	Value
No. Of Computers	60
No. Of Workstations	59
Disabled Computers	3
Domain Controllers	1

Inside ADManager Plus

ADManager Plus has a stream of tools to manage Active Directory from anywhere.

Help Desk - Reset Password Console

AD Management

- Account Provisioning (via CSV Import)
- Account Provisioning (Via Templates)
- Account Deprovisioning
- Cleanup Activities(Move/Disable Account)

[more](#)

AD Reports

- Inactive User accounts
- Real Last Logon
- Group membership (including nested members)
- Password Expired users
- Locked Out Users
- IT Compliance reports

[more](#)

Helpdesk Delegation

- Role-based Delegation
- OU-based Administration

ManageEngine ADManager Plus is an AD management tool that allows users to conduct Active Directory management and generate reports. In terms of management capabilities, you can manage AD objects, groups, and users from one location. This is beneficial because it allows you to sidestep the hassle of your Active Directory management and use the sleek ManageEngine GUI instead.

Key Features

- Offers a front end to AD
- Unify the management of many instances
- Compliance reporting
- Easy to navigate

With regards to reports, **ManageEngine ADManager Plus** can be used to automate the report generation process. This means that you can generate reports without having to do everything manually. This not only makes Active Directory management more convenient but also reduces the time that would be wasted on navigating the Active Directory program.

It is also worth mentioning that ManageEngine ADManager Plus is a tool you should consider for regulatory compliance as well. If you need to complete a compliance audit for SOX or HIPAA, the ability to manage your Active Directory data and generate reports is invaluable.

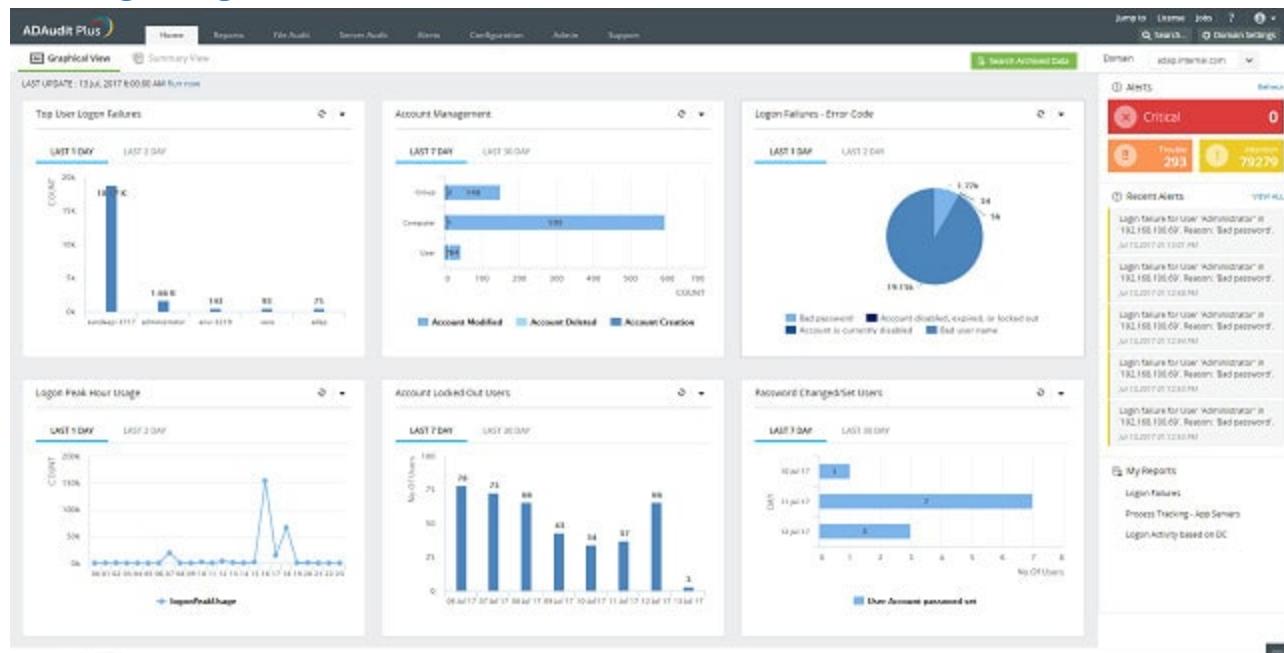
Pros:

- Detailed reporting, can generate compliance reports for all major standards (PCI, HIPAA, etc.)
- Supports multiple domains
- Supports delegation for NOC or helpdesk teams
- Allows you to visually view share permissions and the details of security groups

Price-wise ManageEngine ADManager Plus is available for download on a [30-day free trial](#). We recommend this product to anyone wanting to make Active Directory Management more convenient as well as those who want to benefit from a high-quality report function.

See also: [Access Rights Management Tools](#)

3. ManageEngine ADAudit Plus



AdAudit Plus from ManageEngine has a stronger focus on standards compliance requirements than the company's ADManager Plus tool. This system auditing utility is a powerful AD tool that gives you live user activity reports and includes **automated insider threat detection systems**. You will be able to block people who are allowed access to your resources from using them inappropriately.

Key Features

- Compliance enforcement
- User activity tracking
- Insider threat detection

One of the main reasons that you would be interested in AdAudit Plus is if you need to demonstrate compliance with data protection standards to win or keep service contracts. This tool has a great bundle of pre-formatted standards compliance reports, which follow the **SOX, HIPAA, GLBA, PCI-DSS, and FISMA standards**. So, you won't need to customize the system or set up your own reports in order to demonstrate compliance.

Pros:

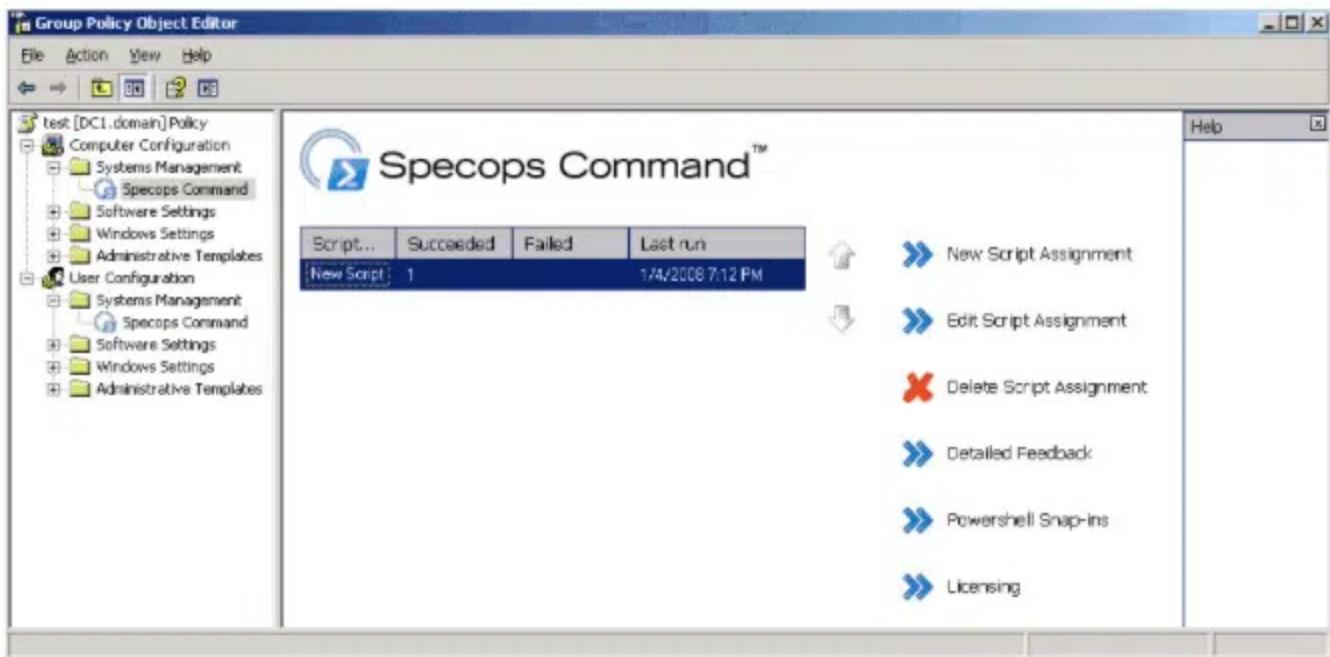
- Focused heavily on compliance requirements, making it a good option for maintaining industry compliance
- Pre-configured compliance reports allow you to see where you stand in just a few clicks
- Features insider threat detection, can detect snooping staff members or blatant malicious actors who have infiltrated the LAN
- Supports automation and scripting
- Great user interface

Cons:

- Upgrading can often break features and cause issues
- Custom reporting has a steep learning curve

ManageEngine produces three editions of AdAudit Plus. These are **Free, Standard, and Professional**. A great offer to look into is the [30-day free trial](#) of the Standard edition. You don't have to enter any payment details to get this offer and you won't be charged automatically when the trial period ends. If you choose not to buy, your installation automatically switches over to the Free edition.

4. Specops Command



Specops Command is another tool that offers you a formidable Active Directory management experience. With this program, you use scripts to manage your network. Specops Command enables the use of Windows PowerShell and VBScripts to manage users and devices throughout your network. You can even execute commands straight through to client systems.

Key Features

- Supports PowerShell and VBScripts functions
- Manages scripts
- Generate AD reports

What makes the scripting feature interesting is that you can not only write your own scripts but import them straight from a file as well. In addition, you can schedule when a script will be executed. This gives you an additional measure of automation that allows you to take a step back.

Not wanting to be a one trick pony, SpecOps Command also allows you to generate reports as well. These reports are web-based and designed around script feedback. The advantage here is you can take extra time to analyze the feedback from what you've done.

Pros:

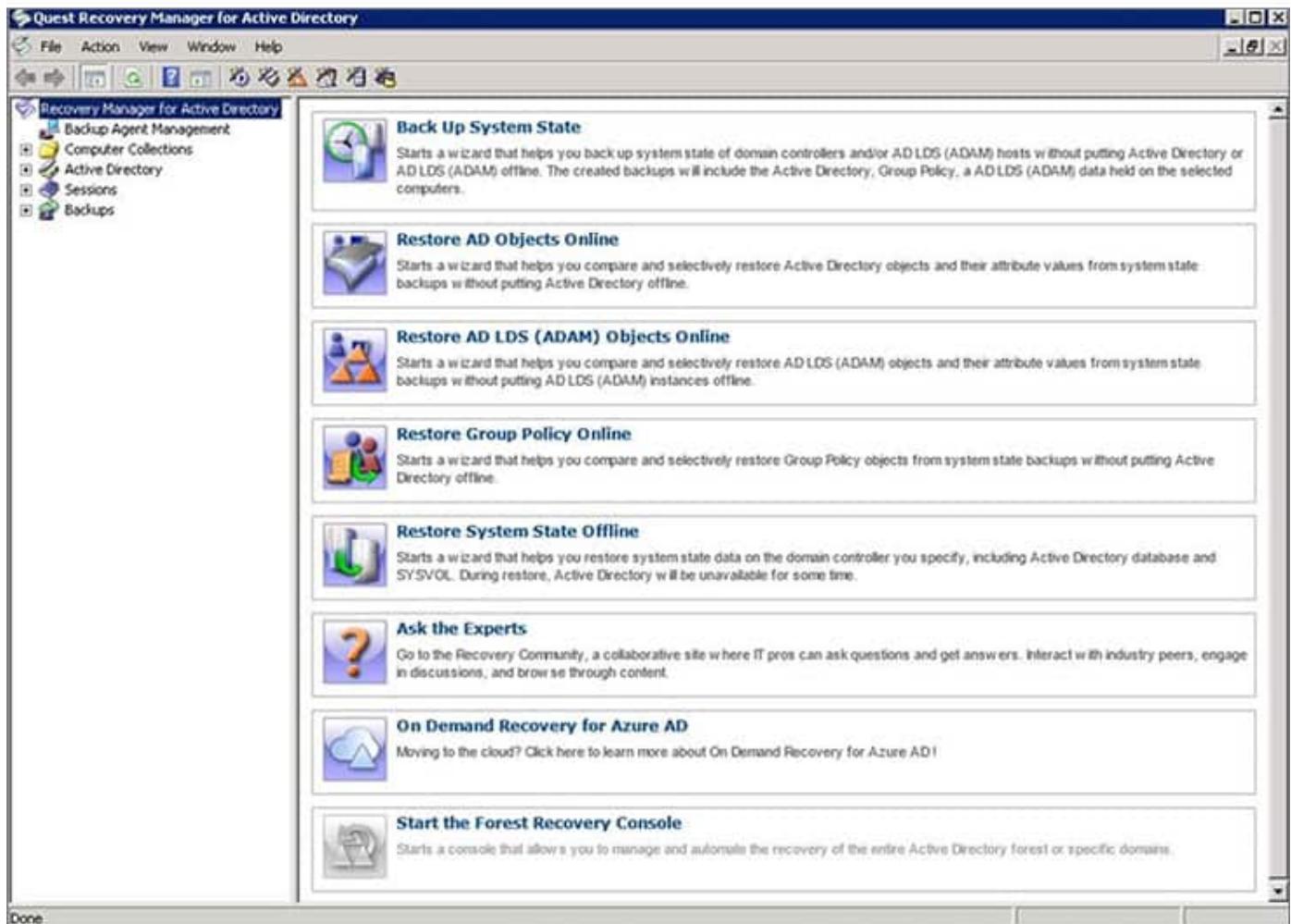
- Extremely lightweight, runs from PowerShell
- Very flexible, allows for VBScript and PowerShell commands
- Can generate reports
- Designed for professionals that want a bare-bones option

Cons:

- Much steeper learning curve than similar tools
- No real graphical interface
- Reporting is limited
- No pre-configured actions or reports

Overall Specops Command is a product that offers a complementary mix of additional features of Active Directory. This product is recommended based on its scripting ability alone, but its support for reports also makes it useful for regulatory compliance as well. Specops Command can be [downloaded for free](#).

5. Recovery Manager for Active Directory



As the name suggests, Recovery for Active Directory is a third-party tool for Active Directory that has been designed to help you recover data. Generally speaking, when an object is lost in Active Directory you have to restart the Domain Controller to recover it. Recovery Manager for Active Directory eliminates this inconvenience by allowing you to recover objects without restarting Active Directory.

Key Features

- Fast recovery of AD objects
- Also operates for Azure
- Visualize hierarchies

With **Recovery Manager for Active Directory** you can **restore objects such as users, computers, attributes, configurations, sites, subnets, group policy objects, and organizational units**. In other words, if you lose something you can recover it.

The advantage of this is far beyond convenience. By allowing you to recover without restarting, your service stays online and any damage done to your service is minimized. Whether the system fails due to a security event or a fault you can get the recovery process started immediately. There is also a reporting process that highlights any changes that have taken place since the last backup. This helps you to see if any undesirable changes have taken place.

However this isn't all, as Recovery Manager for Active Directory also offers you Hybrid and Azure Active Directory Recovery as well. This means you have a wide coverage of basic network infrastructure as much as off-premises services.

Pros:

- Adds helpful graphical elements to AD to enhance the management experience
- Helpful for recovering deleted objects from the graveyard
- Supports Azure AD as well as on premise versions
- Can help visualize permissions and inheritance

Cons:

- Interface feels a bit outdated
- Some of the Wizards aren't as intuitive as other

The only issue with the **Recovery Manager for Active Directory** is that its pricing is not transparent. You have to contact the Quest Sales Department to [get a quote](#). To examine the system, you can download a [30-day free trial](#) – the software installs on **Windows Server**.

6. ManageEngine Free Active Directory Tools

AD Query

AD Query Tool

Domain Name :

Query : **Generate**

Total Number Of Objects : 1323 **Advanced**

NAME	FIRST NAME	INITIAL	LAST NAME	DISPLAY
Administrator	-	-	-	-
Guest	-	-	-	-
krbtgt	-	-	-	-
Johnson Davidson	Johnson	-	Davidson	Johnso
Robert	Robert	cv	-	-
Mathew Raj	Mathew	-	-	Mathe
Charles	Charles	-	-	Charle
Manikandan	Manikandan	v	-	Manikand
Margaret	Margaret	-	-	Margaret
George	George	-	-	George
Stalin	Stalin	-	-	Stalin
Raja	Raja	-	-	Raja
Emily	Emily	-	-	Emily
Gloria	Gloria	-	-	Gloria
Rabycol	Rabycol	-	-	Rabycol
Veronica	Veronica	-	Veronica	Veronica
Joel	Joel	-	-	Joel
Sophy	Sophy	-	-	Sophy
Mark Antony	Mark	-	Antony	Mark
Victor	Victor	-	-	Victor

Copyright © 2015 ZOHO Corp. All rights reserved | Looking for more reports? www.admanagerplus.com

ManageEngine Free Active Directory Tools is essentially a group of utilities that help to manage Active Directory. Some of the utilities available include AD Query Tool, CSV Generator, Last Logon Reporter, Terminal Session Manager, AD Replication Manager, SharePoint Manager, DMZ Port Analyzer, Domain and DC Roles Reported, Local Users Manager, Password Policy Manager, and Exchange Health Monitor.

Key Features

- A bundle of 14 tools
- Password renewal reminder
- See who is connected

All of these utilities have the focus of making it easier to manage Active Directory. For example, there is a **Free Password Expiry Notifier utility** that **reminds users to update their passwords via email or SMS**. Similarly, the Duplicates Identifier allows you to see all duplicated objects in one click. The result is an **Active Directory** administrative experience that is more versatile than **Active Directory** alone.

Another interesting utility is the Terminal Session Manager. With the Terminal Session Manager the user can utilize a PowerShell cmdlet to find and manage a range of terminal sessions from a centralized location. This is particularly useful because it allows you to manage and disconnect multiple users from one location.

Pros:

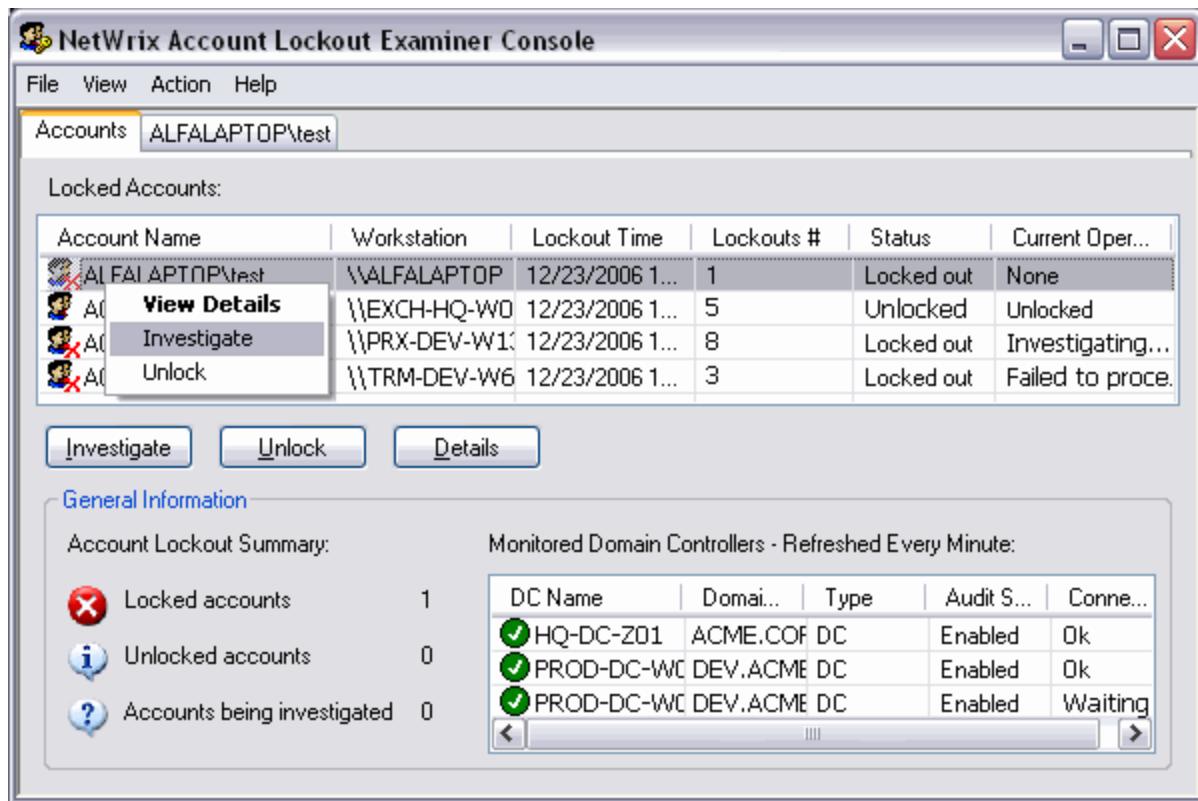
- A complete tool set of over 14 different tools that add additional functionality into Active Directory
- Can be notified when an AD account password is locked out, or going to expire soon
- Offers a duplicate objects finder, great for cleaning up larger directories
- Can export lists of members based on permissions, group, or name
- Completely free

Cons:

- Different functionality is found in different tools, it would be more convenient to have most features in a single tool
- Some tools come with little explanation of how to use them

The ManageEngine Free Active Directory Tools bundle is well worth considering if you're looking to add a range of new Active Directory functions to your tricks bag. One of the best things about this is that you won't have to pay for the privilege of these utilities either because [everything is free to download](#).

7. Netwrix Account Lockout Examiner



There are many occasions in Active Directory where a user is locked out of Active Directory at the most inconvenient time. Netwrix Account Lockout Examiner has been designed for the expressed purpose of getting to the bottom of Active Directory lockouts. This tool notifies administrators when an account has been locked out of Active Directory so that they can take a closer look at why this is the case.

Key Features

- Fast identification of locked accounts
- Unlock button
- Investigation option

You can use **Netwrix Account Lockout Examiner** to ascertain why the user has been locked out with relative ease. Whether it's on account of a disconnected desktop or a task obscuring the service you will be able to tell. This allows you to tell if you need to take further action or if it's a temporary blip.

Once an administrator has seen that an account has been locked out they can unlock that account through the centralized console or a mobile device. This enables the user to get user accounts unlocked ASAP. As a consequence, normal service can be resumed much quicker than it would be trying to go it alone with Active Directory.

Pros:

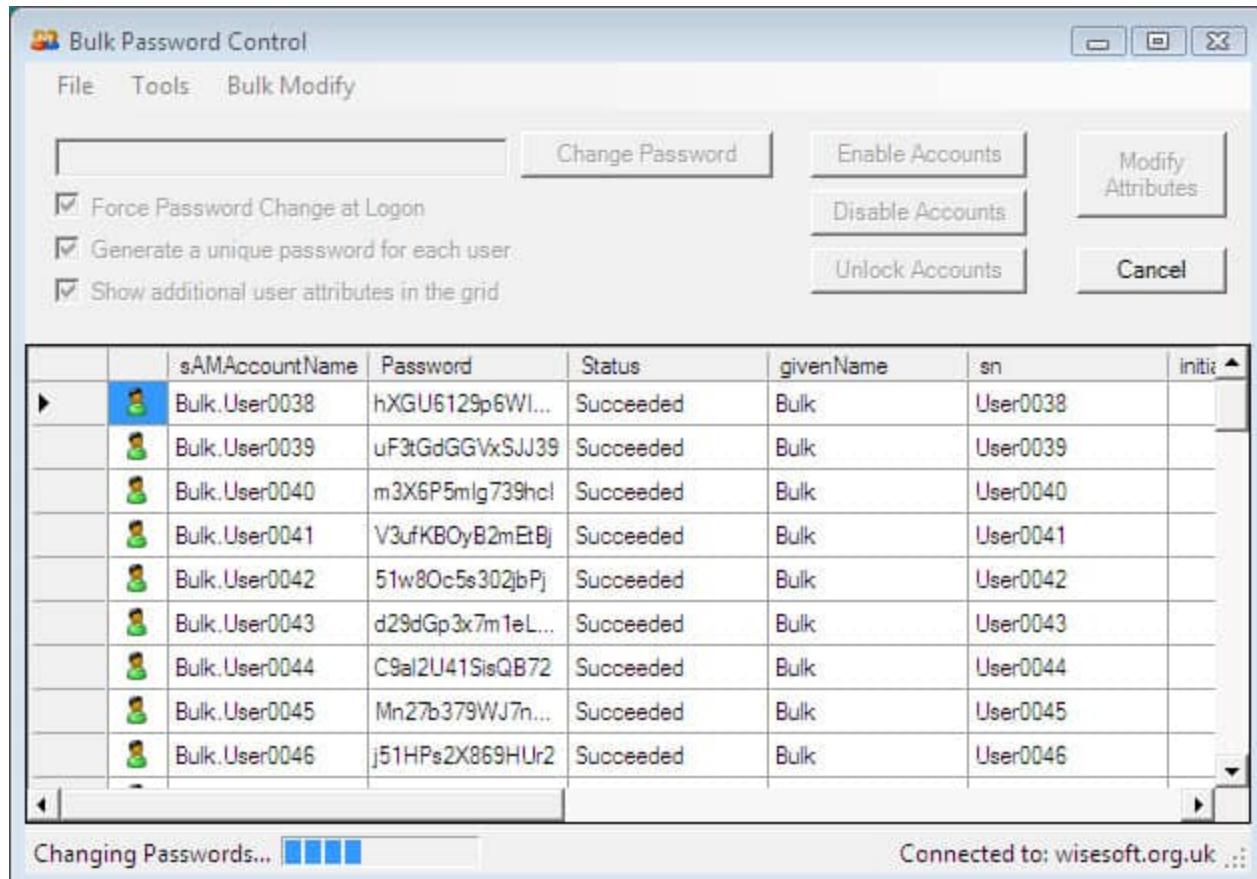
- Provides a visual indication of when accounts are locked, great for detecting attempted attacks
- Can unlock accounts directly from the tool without reopening ADUC
- Can investigate netlogon for more details from within the tool
- Completely free

Cons:

- Interface is a bit cluttered, not viable for tracking a large number of users
- May have to refresh the program to see new lockouts

Netwrix Account Lockout Examiner is a tool that provides a solid account monitoring experience. In the event that a user gets locked out this tool is invaluable at getting the account unlocked so that they can get back to business quickly. This product can be [downloaded for free](#).

8. Bulk Password Control



Bulk Password Control is a tool designed to help users with password management on **Active Directory**. As a password manager, **Bulk Password Control** is very fast paced. You can **change passwords on multiple accounts at once**. You can do this through the use of a **password generator** that creates passwords for each account. In the event that you want to make this more simple, you can set every account password to the same code. In other words, you can manage passwords in bulk.

Key Features

- Mass password setting
- Password generator
- Enable, disable, and unlock accounts

However you aren't limited to resetting passwords for user accounts either; you can also unlock, enable or disable user accounts as well. This gives you a high degree of control over your active directory users and computers so that if you need to restructure or remove an unsuitable account you can do so with ease.

Pros:

- Can help manage generic accounts easily
- Saves a ton of time when changing passwords in bulk
- Supports unlocking/locking accounts as well as disabling users
- Free to use

Cons:

- Passwords are visible all in one place, could be a security issue if users are not prompted to reset upon login

The bulk password management ability of this product makes it ideal for larger enterprise environments with lots of different users and accounts. Bulk Password Control can be [downloaded for free](#).

9. Netwrix Inactive User Tracker

Inactive users analysis for Domain enterprise.local completed successfully			
The following accounts are no longer active:			
Account Name	E-Mail	Inactivity Time	Account Age
BBrown	BBrown@enterprise.com	228 day (s)	247 day (s)
LBlack	LBlack@enterprise.com	203 day (s)	239 day (s)
CMorisson	CMorisson@enterprise.com	never logged in	212 day (s)
BCliff	BCliff@enterprise.com	never logged in	147 day (s)

Netwrix Inactive User Tracker is a tool that is used to flag up Active Directory accounts that aren't in use and helps to put them to rest. This tool scans for inactive user accounts and then provides you with information on for how long the accounts have been dormant. In effect, the tool automatically keeps you updated on the state of your connected accounts so that you can take action if need be.

Key Features

- Discovers inactive accounts
- Account activity details
- Auditing features

Once you can see that an account has been inactive for a substantial length of time you can deactivate it. Deactivating inactive accounts will reduce the risk of a malicious entity gaining access to your data. Likewise, it will also help if you are audited because it shows that you are taking a proactive approach towards cybersecurity and record management.

Pros:

- Can easily see metrics like last login, account age, and username from a single space
- Good for pruning inactive accounts and identifying potential security flaws
- Can quickly identify modified/new accounts that could be malicious

Netwrix Inactive User Tracker is a tool that is worth its weight in gold for those moments where you need to clean up your Active Directory accounts. Doing this regularly will not only get rid of records you don't need but will also eliminate vulnerable accounts that can be accessed for malicious purposes. Netwrix Inactive User Tracker can be [downloaded for free](#).