Windows Server Built-in Groups

Enterprise Admins

The Enterprise Admins (EA) group is located in the forest root domain, and by default, it is a member of the built-in Administrators group in every domain in the forest. The Built-in Administrator account in the forest root domain is the only default member of the EA group. EAs are granted rights and permissions that allow them to affect forest-wide changes. These are changes that affect all domains in the forest, such as adding or removing domains, establishing forest trusts, or raising forest functional levels. In a properly designed and implemented delegation model, EA membership is required only when first constructing the forest or when making certain forest-wide changes such as establishing an outbound forest trust.

The EA group is located by default in the Users container in the forest root domain, and it is a universal security group, unless the forest root domain is running in Windows 2000 Server mixed mode, in which case the group is a global security group. Although some rights are granted directly to the EA group, many of this group's rights are actually inherited by the EA group because it is a member of the Administrators group in each domain in the forest. Enterprise Admins have no default rights on workstations or member servers.

Domain Admins

Each domain in a forest has its own Domain Admins (DA) group, which is a member of that domain's built-in Administrators (BA) group in addition to a member of the local Administrators group on every computer that is joined to the domain. The only default member of the DA group for a domain is the Built-in Administrator account for that domain.

DAs are all-powerful within their domains, while EAs have forest-wide privilege. In a properly designed and implemented delegation model, DA membership should be required only in "break glass" scenarios, which are situations in which an account with high levels of privilege on every computer in the domain is needed, or when certain domain wide changes must be made. Although native Active Directory delegation mechanisms do allow delegation to the extent that it is possible to use DA accounts only in emergency scenarios, constructing an effective delegation model can be time consuming, and many organizations use third-party applications to expedite the process.

The DA group is a global security group located in the Users container for the domain. There is one DA group for each domain in the forest, and the only default member of a DA group is the domain's Built-in Administrator account. Because a domain's DA group is nested in the domain's BA group and every domain-joined system's local Administrators group, DAs not only have permissions that are specifically granted to Domain Admins, but they also inherit all rights and permissions granted to the domain's Administrators group and the local Administrators group on all systems joined to the domain.

Administrators

The built-in Administrators (BA) group is a domain local group in a domain's Built-in container into which DAs and EAs are nested, and it is this group that is granted many of the direct rights and permissions in the directory and on domain controllers. However, the Administrators group for a domain does not have any privileges on member servers or on workstations. Membership in domain-joined computers' local Administrators group is where local privilege is granted; and of the groups discussed, only DAs are members of all domain-joined computers' local Administrators groups by default.

The Administrators group is a domain-local group in the domain's Built-in container. By default, every domain's BA group contains the local domain's Built-in Administrator account, the local domain's DA group, and the forest root domain's EA group. Many user rights in Active Directory and on domain controllers are granted specifically to the Administrators group, not to EAs or DAs. A domain's BA group is granted full control permissions on most directory objects, and can take ownership of directory objects. Although EA and DA groups are granted certain object-specific permissions in the forest and domains, much of the power of groups is actually "inherited" from their membership in BA groups.

Schema Admins

The Schema Admins (SA) group is a universal group in the forest root domain and has only that domain's Built-in Administrator account as a default member, similar to the EA group. Although membership in the SA group can allow an attacker to compromise the Active Directory schema, which is the framework for the entire Active Directory forest, SAs have few default rights and permissions beyond the schema.

You should carefully manage and monitor membership in the SA group, but in some respects, this group is "less privileged" than the three highest privileged groups described earlier because the scope of its privilege is very narrow; that is, SAs have no administrative rights anywhere other than the schema.

Access Control Assistance Operators (Active Directory in Windows Server 2012)

Members of this group can remotely query authorization attributes and permissions for resources on this computer.

Inherited user rights:

- Access this computer from the network
- Add workstations to domain
- Bypass traverse checking
- Increase a process working set

Account Operators

Members can administer domain user and group accounts.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

Administrator account

Built-in account for administering the domain.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Adjust memory quotas for a process
- ✓ Allow log on locally
- ✓ Allow log on through Remote Desktop Services
- ✓ Back up files and directories
- ✓ Bypass traverse checking
- ✓ Change the system time
- ✓ Change the time zone
- ✓ Create a pagefile
- ✓ Create global objects
- ✓ Create symbolic links
- ✓ Debug programs
- ✓ Enable computer and user accounts to be trusted for delegation
- ✓ Force shutdown from a remote system
- ✓ Impersonate a client after authentication
- ✓ Increase a process working set
- ✓ Increase scheduling priority
- ✓ Load and unload device drivers
- ✓ Log on as a batch job
- ✓ Manage auditing and security log
- ✓ Modify firmware environment values
- ✓ Perform volume maintenance tasks
- ✓ Profile single process
- ✓ Profile system performance
- ✓ Remove computer from docking station
- ✓ Restore files and directories
- ✓ Shut down the system
- ✓ Take ownership of files or other objects

Administrators group

Administrators have complete and unrestricted access to the domain.

Direct user rights:

- ✓ Access this computer from the network
- ✓ Adjust memory quotas for a process
- ✓ Allow log on locally
- ✓ Allow log on through Remote Desktop Services
- ✓ Back up files and directories
- ✓ Bypass traverse checking
- ✓ Change the system time
- ✓ Change the time zone

- ✓ Create a pagefile
- ✓ Create global objects
- ✓ Create symbolic links
- ✓ Debug programs
- ✓ Enable computer and user accounts to be trusted for delegation
- ✓ Force shutdown from a remote system
- ✓ Impersonate a client after authentication
- ✓ Increase scheduling priority
- ✓ Load and unload device drivers
- ✓ Log on as a batch job
- ✓ Manage auditing and security log
- ✓ Modify firmware environment values
- ✓ Perform volume maintenance tasks
- ✓ Profile single process
- ✓ Profile system performance
- ✓ Remove computer from docking station
- ✓ Restore files and directories
- ✓ Shut down the system
- ✓ Take ownership of files or other objects

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

Allowed RODC Password Replication Group

Members in this group can have their passwords replicated to all read-only domain controllers in the domain.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

Backup Operators

Backup Operators can override security restrictions for the sole purpose of backing up or restoring files.

Direct user rights:

- ✓ Allow log on locally
- ✓ Back up files and directories
- ✓ Log on as a batch job
- ✓ Restore files and directories
- ✓ Shut down the system

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

Cert Publishers

Members of this group are permitted to publish certificates to the directory.
Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

Certificate Service DCOM Access

If Certificate Services is installed on a domain controller (not recommended), this group grants DCOM enrollment access to Domain Users and Domain Computers.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

Cloneable Domain Controllers (AD DS in Windows Server 2012AD DS)

Members of this group that are domain controllers may be cloned.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

Cryptographic Operators

Members are authorized to perform cryptographic operations.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

Denied RODC Password Replication Group

Members in this group cannot have their passwords replicated to any read-only domain controllers in the domain.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

DHCP Administrators

Members of this group have administrative access to the DHCP Server service.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

DHCP Users

Members of this group have view-only access to the DHCP Server service.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

Distributed COM Users

Members of this group are allowed to launch, activate, and use distributed COM objects on this computer.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

DnsAdmins

Members of this group have administrative access to the DNS Server service.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

DnsUpdateProxy

Members of this group are DNS clients who are permitted to perform dynamic updates on behalf of clients that cannot themselves perform dynamic updates. Members of this group are typically DHCP servers.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

Domain Admins

Designated administrators of the domain; Domain Admins is a member of every domain-joined computer's local Administrators group and receives rights and permissions granted to the local Administrators group, in addition to the domain's Administrators group.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Adjust memory quotas for a process
- ✓ Allow log on locally
- ✓ Allow log on through Remote Desktop Services
- ✓ Back up files and directories
- ✓ Bypass traverse checking
- ✓ Change the system time
- ✓ Change the time zone
- ✓ Create a pagefile
- ✓ Create global objects
- ✓ Create symbolic links
- ✓ Debug programs
- ✓ Enable computer and user accounts to be trusted for delegation
- ✓ Force shutdown from a remote system
- ✓ Impersonate a client after authentication
- ✓ Increase a process working set
- ✓ Increase scheduling priority
- ✓ Load and unload device drivers
- ✓ Log on as a batch job
- ✓ Manage auditing and security log
- ✓ Modify firmware environment values
- ✓ Perform volume maintenance tasks
- ✓ Profile single process
- ✓ Profile system performance
- ✓ Remove computer from docking station
- ✓ Restore files and directories

- ✓ Shut down the system
- ✓ Take ownership of files or other objects

Domain Computers

All workstations and servers that are joined to the domain are by default members of this group.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

Domain Controllers

All domain controllers in the domain. Note: Domain controllers are not a member of the Domain Computers group.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

Domain Guests

All guests in the domain

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

Domain Users

All users in the domain

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

Enterprise Admins (exists only in forest root domain)

Enterprise Admins have permissions to change forest-wide configuration settings; Enterprise Admins is a member of every domain's Administrators group and receives rights and permissions granted to that group.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Adjust memory quotas for a process
- ✓ Allow log on locally
- ✓ Allow log on through Remote Desktop Services
- ✓ Back up files and directories
- ✓ Bypass traverse checking
- ✓ Change the system time
- ✓ Change the time zone
- ✓ Create a pagefile
- ✓ Create global objects
- ✓ Create symbolic links
- ✓ Debug programs
- ✓ Enable computer and user accounts to be trusted for delegation
- ✓ Force shutdown from a remote system
- ✓ Impersonate a client after authentication
- ✓ Increase a process working set
- ✓ Increase scheduling priority
- ✓ Load and unload device drivers
- ✓ Log on as a batch job
- ✓ Manage auditing and security log
- ✓ Modify firmware environment values
- ✓ Perform volume maintenance tasks
- ✓ Profile single process
- ✓ Profile system performance
- ✓ Remove computer from docking station
- ✓ Restore files and directories
- ✓ Shut down the system
- ✓ Take ownership of files or other objects

Enterprise Read-only Domain Controllers

This group contains the accounts for all read-only domain controllers in the forest.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

Event Log Readers

Members of this group in can read the event logs on domain controllers.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

Group Policy Creator Owners

Members of this group can create and modify Group Policy Objects in the domain.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

Guest

This is the only account in an AD DS domain that does not have the Authenticated Users SID added to its access token. Therefore, any resources that are configured to grant access to the Authenticated Users group will not be accessible to this account. This behavior is not true of members of the Domain Guests and Guests groups, however- members of those groups do have the Authenticated Users SID added to their access tokens.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Bypass traverse checking
- ✓ Increase a process working set

Guests

Guests have the same access as members of the Users group by default, except for the Guest account, which is further restricted as described earlier.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

Hyper-V Administrators

Members of this group have complete and unrestricted access to all features of Hyper-V.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

IIS_IUSRS

Built-in group used by Internet Information Services.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

Incoming Forest Trust Builders (exists only in forest root domain)

Members of this group can create incoming, one-way trusts to this forest. (Creation of outbound forest trusts is reserved for Enterprise Admins.)

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

Krbtgt

The Krbtgt account is the service account for the Kerberos Key Distribution Center in the domain. This account has access to all accounts' credentials stored in Active Directory. This account is disabled by default and should never be enabled

Network Configuration Operators

Members of this group are granted privileges that allow them to manage configuration of networking features.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

Performance Log Users
Members of this group can schedule logging of performance counters, enable trace providers, and collect event traces locally and via remote access to the computer.

Direct user rights:

- ✓ Log on as a batch job

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

Performance Monitor Users
Members of this group can access performance counter data locally and remotely.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

Pre-Windows 2000 Compatible Access
This group exists for backward compatibility with operating systems prior to Windows 2000 Server, and it provides the ability for members to read user and group information in the domain.

Direct user rights:

- ✓ Access this computer from the network
- ✓ Bypass traverse checking

Inherited user rights:

- ✓ Add workstations to domain
- ✓ Increase a process working set

Print Operators
Members of this group can administer domain printers.
Direct user rights:

- ✓ Allow log on locally
- ✓ Load and unload device drivers
- ✓ Shut down the system

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

RAS and IAS Servers

Servers in this group can read remote access properties on user accounts in the domain.
Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

RDS Endpoint Servers

Servers in this group run virtual machines and host sessions where users RemoteApp programs and personal virtual desktops run. This group needs to be populated on servers running RD Connection Broker. RD Session Host servers and RD Virtualization Host servers used in the deployment need to be in this group.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

RDS Management Servers

Servers in this group can perform routine administrative actions on servers running Remote Desktop Services. This group needs to be populated on all servers in a Remote Desktop Services deployment. The servers running the RDS Central Management service must be included in this group.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

RDS Remote Access Servers

Servers in this group enable users of RemoteApp programs and personal virtual desktops access to these resources. In Internet-facing deployments, these servers are typically deployed in an edge network. This group needs to be populated on servers running RD Connection Broker. RD Gateway servers and RD Web Access servers used in the deployment need to be in this group.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

Read-only Domain Controllers

This group contains all read-only domain controllers in the domain.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

Remote Desktop Users

Members of this group are granted the right to log on remotely using RDP.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

Remote Management Users

Members of this group can access WMI resources over management protocols (such as WS-Management via the Windows Remote Management service). This applies only to WMI namespaces that grant access to the user.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

Replicator

Supports legacy file replication in a domain.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

Schema Admins (exists only in forest root domain)

Schema admins are the only users who can make modifications to the Active Directory schema, and only if the schema is write-enabled.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

Server Operators
Members of this group can administer domain servers.

Direct user rights:

- ✓ Allow log on locally
- ✓ Back up files and directories
- ✓ Change the system time
- ✓ Change the time zone
- ✓ Force shutdown from a remote system
- ✓ Restore files and directories
- ✓ Shut down the system

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

Terminal Server License Servers
Members of this group can update user accounts in Active Directory with information about license issuance, for the purpose of tracking and reporting TS Per User CAL usage

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

Users
Users have permissions that allow them to read many objects and attributes in Active Directory, although they cannot change most. Users are prevented from making accidental or intentional system-wide changes and can run most applications.

Direct user rights:

- ✓ Increase a process working set

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking

Windows Authorization Access Group
Members of this group have access to the computed tokenGroupsGlobalAndUniversal attribute on User objects

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set

WinRMRemoteWMIUsers
Members of this group can access WMI resources over management protocols (such as WS-Management via the Windows Remote Management service). This applies only to WMI namespaces that grant access to the user.

Inherited user rights:

- ✓ Access this computer from the network
- ✓ Add workstations to domain
- ✓ Bypass traverse checking
- ✓ Increase a process working set