https://web.archive.org/learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups May 30, 2025 at 12:18 PM CDT

https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-grou Go MAR MAY JUN
83 captures 21
28 Sep 2022 – 24 May 2025 2022 2023 2024 About this capture

OpenAI President & Co-Founder Greg Brockman LIVE in Seattle!

Microsoft Build

May 23-25, 2023

Register now >

Filter by title

Identity and Access
Solutions and Scenario Guides
Active Directory Domain Services
Active Directory Domain Services
What's new in Active Directory Domain Services
AD DS Getting started
AD DS Design and Planning
AD DS Deployment
AD DS Operations
AD DS Operations
AD Forest Recovery Guide
Best Practices for Securing Active Directory
Active Directory Replication and Topology Management Using Windows PowerShell
Managing RID issuance
Active Directory Domain Services component updates
Active Directory accounts
Special identities
Active Directory security groups
Service accounts

Active Directory security groups

Article • 04/10/2023 • 4 contributors Feedback

In this article

What is a security group in Active Directory?
How Active Directory security groups work
Default security groups
See also

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Learn about default Active Directory security groups, group scope, and group functions.

What is a security group in Active Directory?

Active Directory has two forms of common security principals: user accounts and computer accounts. These accounts represent a physical entity that is either a person or a computer. A user account also can be used as a dedicated service account for some applications.

Security groups are a way to collect user accounts, computer accounts, and other groups into manageable units.

IPR2025-01086
Orca Security EX1021 Page 1

In the Windows Server operating system, several built-in accounts and security groups are preconfigured with the appropriate rights and permissions to perform specific tasks. In Active Directory, administrative responsibilities are separated into two types of administrators:

- **Service administrators**: Responsible for maintaining and delivering Active Directory Domain Services (AD DS), including managing domain controllers and configuring AD DS.
- **Data administrators**: Responsible for maintaining the data that's stored in AD DS and on domain member servers and workstations.

How Active Directory security groups work

Use groups to collect user accounts, computer accounts, and other groups into manageable units. Working with groups instead of with individual users helps you simplify network maintenance and administration.

Active Directory has two types of groups:

- **Security groups**: Use to assign permissions to shared resources.
- **Distribution groups**: Use to create email distribution lists.

Security groups

Security groups can provide an efficient way to assign access to resources on your network. By using security groups, you can:

- Assign user rights to security groups in Active Directory.

  Assign user rights to a security group to determine what members of that group can do within the scope of a domain or forest. User rights are automatically assigned to some security groups when Active Directory is installed to help administrators define a person's administrative role in the domain.

  For example, a user who you add to the Backup Operators group in Active Directory can back up and restore files and directories that are located on each domain controller in the domain. The user can complete these actions because, by default, the user rights *Backup files and directories* and *Restore files and directories* are automatically assigned to the Backup Operators group. Therefore, members of this group inherit the user rights that are assigned to that group.

  You can use Group Policy to assign user rights to security groups to delegate specific tasks. For more information about using Group Policy,

see User Rights Assignment.

- Assign permissions to security groups for resources.

  Permissions are different from user rights. Permissions are assigned to a security group for a shared resource. Permissions determine who can access the resource and the level of access, such as Full control or Read. Some permissions that are set on domain objects are automatically assigned to allow various levels of access to default security groups like the Account Operators group or the Domain Admins group.

  Security groups are listed in Discretionary Access Control Lists (DACLs) that define permissions on resources and objects. When administrators assign permissions for resources like file shares or printers, they should assign those permissions to a security group instead of to individual users. The permissions are assigned once to the group instead of multiple times to each individual user. Each account that's added to a group receives the rights that are assigned to that group in Active Directory. The user receives permissions that are defined for that group.

You can use a security group as an email entity. Sending an email message to a security group sends the message to all the members of the group.

Distribution groups

You can use distribution groups only to send email to collections of users by using an email application like Exchange Server. Distribution groups aren't security enabled, so you can't include them in DACLs.

Group scope

Each group has a scope that identifies the extent to which the group is applied in the domain tree or forest. The scope of a group defines where in the network permissions can be granted for the group. Active Directory defines the following three group scopes:

- Universal
- Global
- Domain Local

> **Note**
>
> In addition to these three scopes, the default groups in the Builtin container have a group scope of Builtin Local. This group scope and group type can't be changed.

The following table describes the three group scopes and how they work as

security groups:

Scope	Possible members	Scope conversion	Can grant permissions	Possible member of
Universal	Accounts from any domain in the same forest Global groups from any domain in the same forest Other Universal groups from any domain in the same forest	Can be converted to Domain Local scope if the group isn't a member of any other Universal group Can be converted to Global scope if the group doesn't contain any other Universal group	On any domain in the same forest or trusting forests	Other Universal groups in the same forest Domain Local groups in the same forest or trusting forests Local groups on computers in the same forest or trusting forests
Global	Accounts from the same domain Other Global groups from the same domain	Can be converted to Universal scope if the group isn't a member of any other Global group	On any domain in the same forest, or trusting domains or forests	Universal groups from any domain in the same forest Other Global groups from the same domain Domain Local groups from any domain in the same forest, or from any trusting domain
Domain Local	Accounts from any domain or any trusted domain Global groups from any domain or any trusted domain Universal groups from any domain in the same forest Other Domain Local groups from the same domain Accounts, Global groups, and Universal groups from other forests and from	Can be converted to Universal scope if the group doesn't contain any other Domain Local group	Within the same domain	Other Domain Local groups from the same domain Local groups on computers in the same domain, excluding built-in groups that have well-known security identifiers (SIDs)

external
domains

Special identity groups

Special identities are referred to as groups. Special identity groups don't have specific memberships that you can modify, but they can represent different users at different times depending on the circumstances. Some of these groups include Creator Owner, Batch, and Authenticated User.

For more information, see Special identity groups.

Default security groups

Default groups like the Domain Admins group are security groups that are created automatically when you create an Active Directory domain. You can use these predefined groups to help control access to shared resources and to delegate specific domain-wide administrative roles.

Many default groups are automatically assigned a set of user rights that authorize members of the group to perform specific actions in a domain, like logging on to a local system or backing up files and folders. For example, a member of the Backup Operators group can perform backup operations for all domain controllers in the domain.

When you add a user to a group, the user receives all the user rights that are assigned to the group, including all the permissions that are assigned to the group for any shared resources.

Default groups are located in the Builtin container and in the Users container in Active Directory Users and Computers. The Builtin container includes groups that are defined with the Domain Local scope. The Users container includes groups that are defined with Global scope and groups that are defined with Domain Local scope. You can move groups that are located in these containers to other groups or organizational units within the domain, but you can't move them to other domains.

Some of the administrative groups that are listed in this article and all members of these groups are protected by a background process that periodically checks for and applies a specific security descriptor. This descriptor is a data structure that contains security information that's associated with a protected object. This process ensures that any successful unauthorized attempt to modify the security descriptor on one of the administrative accounts or groups is overwritten with the protected settings.

The security descriptor is present on the AdminSDHolder object. If you want to modify the permissions on one of the service administrator groups or on any of its member accounts, you must modify the security descriptor on the

AdminSDHolder object so that it's applied consistently. Be careful when you make these modifications because you're also changing the default settings that are applied to all your protected administrative accounts.

Default Active Directory security groups

The following list provides descriptions of the default groups that are located in the Builtin and Users containers in Active Directory:

- Access Control Assistance Operators
- Account Operators
- Administrators
- Allowed RODC Password Replication
- Backup Operators
- Certificate Service DCOM Access
- Cert Publishers
- Cloneable Domain Controllers
- Cryptographic Operators
- Denied RODC Password Replication
- Device Owners
- DHCP Administrators
- DHCP Users
- Distributed COM Users
- DnsUpdateProxy
- DnsAdmins
- Domain Admins
- Domain Computers
- Domain Controllers
- Domain Guests
- Domain Users
- Enterprise Admins
- Enterprise Key Admins
- Enterprise Read-only Domain Controllers
- Event Log Readers
- Group Policy Creator Owners
- Guests
- Hyper-V Administrators
- IIS_IUSRS
- Incoming Forest Trust Builders
- Key Admins
- Network Configuration Operators
- Performance Log Users
- Performance Monitor Users
- Pre–Windows 2000 Compatible Access
- Print Operators
- Protected Users
- RAS and IAS Servers

- RDS Endpoint Servers
- RDS Management Servers
- RDS Remote Access Servers
- Read-only Domain Controllers
- Remote Desktop Users
- Remote Management Users
- Replicator
- Schema Admins
- Server Operators
- Storage Replica Administrators
- System Managed Accounts
- Terminal Server License Servers
- Users
- Windows Authorization Access
- WinRMRemoteWMIUsers_

Access Control Assistance Operators

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

The Access Control Assistance Operators group applies to the Windows Server operating system listed in the Default Active Directory security groups table.

Attribute	Value
Well-known SID/RID	S-1-5-32-579
Type	Builtin Local
Default container	CN=Builtin, DC=<domain>, DC=
Default members	None
Default member of	None
Protected by AdminSDHolder?	No
Safe to move out of default container?	Can't be moved
Safe to delegate management of this group to non-service admins?	
Default user rights	None

Account Operators

The Account Operators group grants limited account creation privileges to a user. Members of this group can create and modify most types of accounts, including accounts for users, Local groups, and Global groups. Group members can log in locally to domain controllers.

Members of the Account Operators group can't manage the Administrator user account, the user accounts of administrators, or the Administrators, Server Operators, Account Operators, Backup Operators, or Print Operators groups. Members of this group can't modify user rights.

The Account Operators group applies to the Windows Server operating system in the Default Active Directory security groups list.

> **Note**
>
> By default, this built-in group has no members. The group can create and manage users and groups in the domain, including its own membership and that of the Server Operators group. This group is considered a service administrator group because it can modify Server Operators, which in turn can modify domain controller settings. As a best practice, leave the membership of this group empty, and don't use it for any delegated administration. This group can't be renamed, deleted, or removed.

Attribute	Value
Well-known SID/RID	S-1-5-32-548
Type	Builtin Local
Default container	CN=Builtin, DC=<domain>, DC=
Default members	None
Default member of	None
Protected by AdminSDHolder?	Yes
Safe to move out of default container?	Can't be moved
Safe to delegate management of this group to non-service admins?	No
Default user rights	Allow log on locally: SeInteractiveLogonRight

Administrators

Members of the Administrators group have complete and unrestricted access to the computer. If the computer is promoted to a domain controller, members of the Administrators group have unrestricted access to the domain.

The Administrators group applies to the Windows Server operating system in the Default Active Directory security groups list.

> **Note**

The Administrators group has built-in capabilities that give its members full control over the system. This group can't be renamed, deleted, or removed. This built-in group controls access to all the domain controllers in its domain, and it can change the membership of all administrative groups. Members of the following groups can modify the Administrators group membership: the default service Administrators, Domain Admins in the domain, and Enterprise Admins. This group has the special privilege to take ownership of any object in the directory or any resource on a domain controller. This account is considered a service administrator group because its members have full access to the domain controllers in the domain.

This security group includes the following changes since Windows Server 2008:

- Default user rights changes: *Allow log on through Terminal Services* existed in Windows Server 2008, and it was replaced by Allow log on through Remote Desktop Services.
- Remove computer from docking station was removed in Windows Server 2012 R2.

Attribute	Value
Well-known SID/RID	S-1-5-32-544
Type	Builtin Local
Default container	CN=Builtin, DC=<domain>, DC=
Default members	Administrator, Domain Admins, Enterprise Admins
Default member of	None
Protected by AdminSDHolder?	Yes
Safe to move out of default container?	Can't be moved
Safe to delegate management of this group to non-service admins?	No
Default user rights	Adjust memory quotas for a process: SeIncreaseQuotaPrivilege Access this computer from the network: SeNetworkLogonRight Allow log on locally: SeInteractiveLogonRight Allow log on through Remote Desktop Services: SeRemoteInteractiveLogonRight Back up files and directories: SeBackupPrivilege Bypass traverse checking: SeChangeNotifyPrivilege

Change the system time: SeSystemTimePrivilege

Change the time zone: SeTimeZonePrivilege

Create a pagefile: SeCreatePagefilePrivilege

Create global objects: SeCreateGlobalPrivilege

Create symbolic links: SeCreateSymbolicLinkPrivilege

Debug programs: SeDebugPrivilege

Enable computer and user accounts to be trusted for delegation: SeEnableDelegationPrivilege

Force shutdown from a remote system: SeRemoteShutdownPrivilege

Impersonate a client after authentication: SeImpersonatePrivilege

Increase scheduling priority: SeIncreaseBasePriorityPrivilege

Load and unload device drivers: SeLoadDriverPrivilege

Log on as a batch job: SeBatchLogonRight

Manage auditing and security log: SeSecurityPrivilege

Modify firmware environment values: SeSystemEnvironmentPrivilege

Perform volume maintenance tasks: SeManageVolumePrivilege

Profile system performance: SeSystemProfilePrivilege

Profile single process: SeProfileSingleProcessPrivilege

Remove computer from docking station: SeUndockPrivilege

Restore files and directories: SeRestorePrivilege

Shut down the system: SeShutdownPrivilege

Take ownership of files or other objects: SeTakeOwnershipPrivilege

Allowed RODC Password Replication

The purpose of this security group is to manage a read-only domain controller (RODC) password replication policy. This group has no members by default, and

it results in the condition that new RODCs don't cache user credentials. The Denied RODC Password Replication group contains various high-privilege accounts and security groups. The Denied RODC Password Replication group supersedes the Allowed RODC Password Replication group.

The Allowed RODC Password Replication group applies to the Windows Server operating system in Default Active Directory security groups.

Attribute	Value
Well-known SID/RID	S-1-5-21-<domain>-571
Type	Domain local
Default container	CN=Users DC=<domain>, DC=
Default members	None
Default member of	None
Protected by AdminSDHolder?	No
Safe to move out of default container?	Can't be moved
Safe to delegate management of this group to non-service admins?	
Default user rights	None

Backup Operators

Members of the Backup Operators group can back up and restore all files on a computer, regardless of the permissions that protect those files. Backup Operators also can log on to and shut down the computer. This group can't be renamed, deleted, or removed. By default, this built-in group has no members, and it can perform backup and restore operations on domain controllers. Members of the following groups can modify Backup Operators group membership: default service Administrators, Domain Admins in the domain, and Enterprise Admins. Members of the Backup Operators group can't modify the membership of any administrative groups. Although members of this group can't change server settings or modify the configuration of the directory, they do have the permissions needed to replace files (including operating system files) on domain controllers. Because members of this group can replace files on domain controllers, they're considered service administrators.

The Backup Operators group applies to the Windows Server operating system in Default Active Directory security groups.

Attribute	Value
Well-known SID/RID	S-1-5-32-551
Type	Builtin Local

Type	Builtin Local
Default container	CN=Builtin, DC=<domain>, DC=
Default members	None
Default member of	None
Protected by AdminSDHolder?	Yes
Safe to move out of default container?	Can't be moved
Safe to delegate management of this group to non-service admins?	No
Default user rights	Allow log on locally: SeInteractiveLogonRight Back up files and directories: SeBackupPrivilege Log on as a batch job: SeBatchLogonRight Restore files and directories: SeRestorePrivilege Shut down the system: SeShutdownPrivilege

Certificate Service DCOM Access

Members of this group can connect to certification authorities in the enterprise.

The Certificate Service DCOM Access group applies to the Windows Server operating system in Default Active Directory security groups.

Attribute	Value
Well-known SID/RID	S-1-5-32-<domain>-574
Type	Domain Local
Default container	CN=Builtin, DC=<domain>, DC=
Default members	None
Default member of	None
Protected by AdminSDHolder?	No
Safe to move out of default container?	Can't be moved
Safe to delegate management of this group to non-service admins?	
Default user rights	None

Cert Publishers

Members of the Cert Publishers group are authorized to publish certificates for User objects in Active Directory.

The Cert Publishers group applies to the Windows Server operating system in Default Active Directory security groups.

Attribute	Value
Well-known SID/RID	S-1-5-21-<domain>-517
Type	Domain Local
Default container	CN=Users, DC=<domain>, DC=
Default members	None
Default member of	Denied RODC Password Replication
Protected by AdminSDHolder?	No
Safe to move out of default container?	Can't be moved
Safe to delegate management of this group to non-service admins?	No
Default user rights	None

Cloneable Domain Controllers

Members of the Cloneable Domain Controllers group that are domain controllers may be cloned. In Windows Server 2012 R2 and Windows Server 2012, you can deploy domain controllers by copying an existing virtual domain controller. In a virtual environment, you no longer have to repeatedly deploy a server image that's prepared by using *Sysprep.exe*, promoting the server to a domain controller, and then complete more configuration requirements for deploying each domain controller (including adding the virtual domain controller to this security group).

For more information, see Introduction to Active Directory Domain Services (AD DS) Virtualization (Level 100).

Attribute	Value
Well-known SID/RID	S-1-5-21-<domain>-522
Type	Global
Default container	CN=Users, DC=<domain>, DC=
Default members	None

Default members	None
Default member of	None
Protected by AdminSDHolder?	No
Safe to move out of default container?	Can't be moved
Safe to delegate management of this group to non-service admins?	
Default user rights	None

Cryptographic Operators

Members of this group are authorized to perform cryptographic operations. This security group was added in Windows Vista Service Pack 1 (SP1) to configure Windows Firewall for IPsec in Common Criteria mode.

The Cryptographic Operators group applies to the Windows Server operating system in Default Active Directory security groups.

This security group was introduced in Windows Vista SP1, and it hasn't changed in subsequent versions.

Attribute	Value
Well-known SID/RID	S-1-5-32-569
Type	Builtin Local
Default container	CN=Builtin, DC=<domain>, DC=
Default members	None
Default member of	None
Protected by AdminSDHolder?	No
Safe to move out of default container?	Can't be moved
Safe to delegate management of this group to non-service admins?	
Default user rights	None

Denied RODC Password Replication

Passwords of members of the Denied RODC Password Replication group can't be replicated to any RODC.

The purpose of this security group is to manage a RODC password replication policy. This group contains various high-privilege accounts and security groups. The Denied RODC Password Replication group supersedes the Allowed RODC

Password Replication group.

This security group includes the following changes since Windows Server 2008:

- Windows Server 2012 changed the default members to include Cert Publishers.

Attribute	Value
Well-known SID/RID	S-1-5-21-<domain>-572
Type	Domain local
Default container	CN=Users, DC=<domain>, DC=
Default members	Cert Publishers Domain Admins Domain Controllers Enterprise Admins Group Policy Creator Owners Read-only Domain Controllers Schema Admins
Default member of	None
Protected by AdminSDHolder?	No
Safe to move out of default container?	
Safe to delegate management of this group to non-service admins?	
Default user rights	None

Device Owners

When the Device Owners group has no members, we recommend that you don't change the default configuration for this security group. Changing the default configuration might hinder future scenarios that rely on this group. The Device Owners group currently isn't used in Windows.

The Device Owners group applies to the Windows Server operating system in Default Active Directory security groups.

Attribute	Value
Well-known SID/RID	S-1-5-32-583
Type	Builtin Local

Default container	CN=Builtin, DC=<domain>, DC=
Default members	None
Default member of	None
Protected by AdminSDHolder?	No
Safe to move out of default container?	You can move the group, but we don't recommend it
Safe to delegate management of this group to non-service admins?	No
Default user rights	Allow log on locally: SeInteractiveLogonRight Access this computer from the network: SeNetworkLogonRight Bypass traverse checking: SeChangeNotifyPrivilege Change the time zone: SeTimeZonePrivilege

DHCP Administrators

Members of the DHCP Administrators group can create, delete, and manage different areas of the server's scope, including the rights to back up and restore the Dynamic Host Configuration Protocol (DHCP) database. Even though this group has administrative rights, it isn't part of the Administrators group because this role is limited to DHCP services.

The DHCP Administrators group applies to the Windows Server operating system in Default Active Directory security groups.

Attribute	Value
Well-known SID/RID	S-1-5-21-<domain>
Type	Builtin Local
Default container	CN=Builtin, DC=<domain>, DC=
Default members	None
Default member of	Users
Protected by AdminSDHolder?	No
Safe to move out of default container?	You can move the group, but we don't recommend it
Safe to delegate management of this group to non-service admins?	No

Default user rights	None

DHCP Users

Members of the DHCP Users group can see which scopes are active or inactive, see which IP addresses are assigned, and view connectivity issues if the DHCP server isn't configured correctly. This group is limited to read-only access to the DHCP server.

The DHCP Users group applies to the Windows Server operating system in Default Active Directory security groups.

Attribute	Value
Well-known SID/RID	S-1-5-21-<domain>
Type	Builtin Local
Default container	CN=Builtin, DC=<domain>, DC=
Default members	None
Default member of	Users
Protected by AdminSDHolder?	No
Safe to move out of default container?	You can move the group, but we don't recommend it
Safe to delegate management of this group to non-service admins?	No
Default user rights	None

Distributed COM Users

Members of the Distributed COM Users group can launch, activate, and use Distributed COM objects on the computer. Microsoft Component Object Model (COM) is a platform-independent, distributed, object-oriented system for creating binary software components that can interact. Distributed Component Object Model (DCOM) allows applications to be distributed across locations that make the most sense to you and to the application. This group appears as an SID until the domain controller is made the primary domain controller and it holds the operations master (also called the *flexible single master operations* or *FSMO*) role.

The Distributed COM Users group applies to the Windows Server operating system in Default Active Directory security groups.

Attribute	Value
Well-known SID/RID	S-1-5-32-562

Type	Builtin Local
Default container	CN=Builtin, DC=<domain>, DC=
Default members	None
Default member of	None
Protected by AdminSDHolder?	No
Safe to move out of default container?	Can't be moved
Safe to delegate management of this group to non-service admins?	
Default user rights	None

DnsUpdateProxy

Members of the DnsUpdateProxy group are DNS clients. They're permitted to perform dynamic updates on behalf of other clients, like for DHCP servers. A DNS server can develop stale resource records when a DHCP server is configured to dynamically register host (A) and pointer (PTR) resource records on behalf of DHCP clients by using dynamic update. Adding clients to this security group mitigates this scenario.

However, to protect against unsecured records or to permit members of the DnsUpdateProxy group to register records in zones that allow only secured dynamic updates, you must create a dedicated user account and configure DHCP servers to perform DNS dynamic updates by using the credentials (username, password, and domain) of this account. Multiple DHCP servers can use the credentials of one dedicated user account. This group exists only if the DNS server role is or was once installed on a domain controller in the domain.

For more information, see DNS record ownership and the DnsUpdateProxy group.

Attribute	**Value**
Well-known SID/RID	S-1-5-21-<domain>-<variable RI>
Type	Global
Default container	CN=Users, DC=<domain>, DC=
Default members	None
Default member of	None
Protected by AdminSDHolder?	No
Safe to move out of default container?	Yes

Safe to delegate management of this group to non-service admins?	
Default user rights	None

DnsAdmins

Members of the DnsAdmins group have access to network DNS information. The default permissions are Allow: Read, Write, Create All Child objects, Delete Child objects, Special Permissions. This group exists only if the DNS server role is or was once installed on a domain controller in the domain.

For more information about security and DNS, see DNSSEC in Windows Server 2012.

Attribute	Value
Well-known SID/RID	S-1-5-21-<domain>-<variable RI>
Type	Builtin Local
Default container	CN=Users, DC=<domain>, DC=
Default members	None
Default member of	None
Protected by AdminSDHolder?	No
Safe to move out of default container?	Yes
Safe to delegate management of this group to non-service admins?	
Default user rights	None

Domain Admins

Members of the Domain Admins security group are authorized to administer the domain. By default, the Domain Admins group is a member of the Administrators group on all computers that have joined a domain, including the domain controllers. The Domain Admins group is the default owner of any object that's created in Active Directory for the domain by any member of the group. If members of the group create other objects, such as files, the default owner is the Administrators group.

The Domain Admins group controls access to all domain controllers in a domain, and it can modify the membership of all administrative accounts in the domain. Members of the service administrator groups in its domain (Administrators and Domain Admins) and members of the Enterprise Admins

group can modify Domain Admins membership. This group is considered a service administrator account because its members have full access to the domain controllers in a domain.

The Domain Admins group applies to the Windows Server operating system in Default Active Directory security groups.

Attribute	Value
Well-known SID/RID	S-1-5-21-<domain>-512
Type	Global
Default container	CN=Users, DC=<domain>, DC=
Default members	Administrator
Default member of	Administrators Denied RODC Password Replication
Protected by AdminSDHolder?	Yes
Safe to move out of default container?	Yes
Safe to delegate management of this group to non-service admins?	No
Default user rights	See Administrators See Denied RODC Password Replication

Domain Computers

This group can include all computers and servers that have joined the domain, excluding domain controllers. By default, any computer account that's created automatically becomes a member of this group.

The Domain Computers group applies to the Windows Server operating system in Default Active Directory security groups.

Attribute	Value
Well-known SID/RID	S-1-5-21-<domain>-515
Type	Global
Default container	CN=Users, DC=<domain>, DC=
Default members	All computers joined to the domain, excluding domain controllers
Default member of	None
Protected by AdminSDHolder?	No

Safe to move out of default container?	Yes (but not required)
Safe to delegate management of this group to non-service admins?	Yes
Default user rights	None

Domain Controllers

The Domain Controllers group can include all domain controllers in the domain. New domain controllers are automatically added to this group.

The Domain Controllers group applies to the Windows Server operating system in Default Active Directory security groups.

Attribute	Value
Well-known SID/RID	S-1-5-21-<domain>-516
Type	Global
Default container	CN=Users, DC=<domain>, DC=
Default members	Computer accounts for all domain controllers of the domain
Default member of	Denied RODC Password Replication
Protected by AdminSDHolder?	Yes
Safe to move out of default container?	No
Safe to delegate management of this group to non-service admins?	No
Default user rights	None

Domain Guests

The Domain Guests group includes the domain's built-in Guest account. When members of this group sign in as local guests on a domain-joined computer, a domain profile is created on the local computer.

The Domain Guests group applies to the Windows Server operating system in Default Active Directory security groups.

Attribute	Value
Well-known SID/RID	S-1-5-21-<domain>-514
Type	Global
Default container	CN=Users, DC=<domain>, DC=
Default members	Guest

Default member of	Guests
Protected by AdminSDHolder?	No
Safe to move out of default container?	You can move the group, but we don't recommend it
Safe to delegate management of this group to non-service admins?	No
Default user rights	See Guests

Domain Users

The Domain Users group includes all user accounts in a domain. When you create a user account in a domain, it's automatically added to this group.

By default, any user account that's created in the domain automatically becomes a member of this group. You can use this group to represent all users in the domain. For example, if you want all domain users to have access to a printer, you can assign permissions for the printer to this group or add the Domain Users group to a Local group on the print server that has permissions for the printer.

The Domain Users group applies to the Windows Server operating system in Default Active Directory security groups.

Attribute	**Value**
Well-known SID/RID	S-1-5-21-<domain>-513
Type	Global
Default container	CN=Users, DC=<domain>, DC=
Default members	Administrator
krbtgt	
Default member of	Users
Protected by AdminSDHolder?	No
Safe to move out of default container?	Yes
Safe to delegate management of this group to non-service admins?	No
Default user rights	See Users

Enterprise Admins

The Enterprise Admins group exists only in the root domain of an Active

Directory forest of domains. The group is a Universal group if the domain is in native mode. The group is a Global group if the domain is in mixed mode. Members of this group are authorized to make forest-wide changes in Active Directory, like adding child domains.

By default, the only member of the group is the Administrator account for the forest root domain. This group is automatically added to the Administrators group in every domain in the forest, and it provides complete access to configuring all domain controllers. Members in this group can modify the membership of all administrative groups. Members of the default service administrator groups in the root domain can modify Enterprise Admins membership. This group is considered a service administrator account.

The Enterprise Admins group applies to the Windows Server operating system in Default Active Directory security groups.

Attribute	Value
Well-known SID/RID	S-1-5-21-<root domain>-519
Type	Universal if domain is in native mode; otherwise, Global
Default container	CN=Users, DC=<domain>, DC=
Default members	Administrator
Default member of	Administrators Denied RODC Password Replication
Protected by AdminSDHolder?	Yes
Safe to move out of default container?	Yes
Safe to delegate management of this group to non-service admins?	No
Default user rights	See Administrators See Denied RODC Password Replication

Enterprise Key Admins

Members of this group can perform administrative actions on key objects within the forest.

Attribute	Value
Well-known SID/RID	S-1-5-21-<domain>-527
Type	Global
Default container	CN=Users, DC=<domain>,

	DC=
Default members	None
Default member of	None
Protected by AdminSDHolder?	Yes
Safe to move out of default container?	Yes
Safe to delegate management of this group to non-service admins?	No
Default user rights	None

Enterprise Read-only Domain Controllers

Members of this group are RODCs in the enterprise. Except for account passwords, an RODC holds all the Active Directory objects and attributes that a writable domain controller holds. However, changes can't be made to the database that's stored on the RODC. Changes must be made on a writable domain controller and then replicated to the RODC.

RODCs address some of the issues that are commonly found in branch offices. These locations might not have a domain controller, or they might have a writable domain controller but not the physical security, network bandwidth, or local expertise to support it.

For more information, see What is a read-only domain controller?

The Enterprise Read-only Domain Controllers group applies to the Windows Server operating system in Default Active Directory security groups.

Attribute	**Value**
Well-known SID/RID	S-1-5-21-<root domain>-498
Type	Universal
Default container	CN=Users, DC=<domain>, DC=
Default members	None
Default member of	None
Protected by AdminSDHolder?	Yes
Safe to move out of default container?	
Safe to delegate management of this group to non-service admins?	
Default user rights	None

Event Log Readers

Members of this group can read event logs from local computers. The group is created when the server is promoted to a domain controller.

The Event Log Readers group applies to the Windows Server operating system in Default Active Directory security groups.

Attribute	Value
Well-known SID/RID	S-1-5-32-573
Type	Domain Local
Default container	CN=Users, DC=<domain>, DC=
Default members	None
Default member of	None
Protected by AdminSDHolder?	No
Safe to move out of default container?	Can't be moved
Safe to delegate management of this group to non-service admins?	
Default user rights	None

Group Policy Creator Owners

This group is authorized to create, edit, and delete Group Policy Objects in the domain. By default, the only member of the group is Administrator.

For information about other features you can use with this security group, see Group Policy overview.

The Group Policy Creator Owners group applies to the Windows Server operating system in Default Active Directory security groups.

Attribute	Value
Well-known SID/RID	S-1-5-21-<domain>-520
Type	Global
Default container	CN=Users, DC=<domain>, DC=
Default members	Administrator
Default member of	Denied RODC Password Replication
Protected by AdminSDHolder?	No

Safe to move out of default container?	No
Safe to delegate management of this group to non-service admins?	No
Default user rights	See Denied RODC Password Replication

Guests

Members of the Guests group have the same access as members of the Users group by default, except that the Guest account has further restrictions. By default, the only member is the Guest account. The Guests group allows occasional or one-time users to sign in with limited privileges to a computer's built-in Guest account.

When a member of the Guests group signs out, the entire profile is deleted. The profile deletion includes everything that's stored in the *%userprofile%* directory, including the user's registry hive information, custom desktop icons, and other user-specific settings. This fact implies that a guest must use a temporary profile to sign in to the system. This security group interacts with the Group Policy setting. *When this security group is enabled, don't log on users that have temporary profiles*. To access this setting, go to **Computer Configuration** > **Administrative Templates** > **System** > **User Profiles**.

> **Note**
>
> A Guest account is a default member of the Guests security group. People who don't have an actual account in the domain can use the Guest account. A user whose account is disabled (but not deleted) can also use the Guest account. The Guest account does not require a password. You can set rights and permissions for the Guest account as in any user account. By default, the Guest account is a member of the built-in Guests group and of the Domain Guests Global group, which allows a user to sign in to a domain. The Guest account is disabled by default, and we recommend that it stay disabled.

The Guests group applies to the Windows Server operating system in Default Active Directory security groups.

Attribute	Value
Well-known SID/RID	S-1-5-32-546
Type	Builtin Local
Default container	CN=Builtin, DC=<domain>, DC=
Default members	Domain Guests

Default member of	None
Protected by AdminSDHolder?	No
Safe to move out of default container?	Can't be moved
Safe to delegate management of this group to non-service admins?	No
Default user rights	None

Hyper-V Administrators

Members of the Hyper-V Administrators group have complete and unrestricted access to all the features in Hyper-V. Adding members to this group helps reduce the number of members required in the Administrators group and further separates access.

> **Note**
>
> Before Windows Server 2012, access to features in Hyper-V was controlled in part by membership in the Administrators group.

Attribute	**Value**
Well-known SID/RID	S-1-5-32-578
Type	Builtin Local
Default container	CN=Builtin, DC=<domain>, DC=
Default members	None
Default member of	None
Protected by AdminSDHolder?	No
Safe to move out of default container?	Can't be moved
Safe to delegate management of this group to non-service admins?	
Default user rights	None

IIS_IUSRS

IIS_IUSRS is a built-in group that's used by Internet Information Services (IIS) beginning with IIS 7. A built-in account and group are guaranteed by the operating system to always have a unique SID. IIS 7 replaces the IUSR_MachineName account and the IIS_WPG group with the IIS_IUSRS group to ensure that the actual names that the new account and group use are never localized. For example, regardless of the language of the Windows operating

localized. For example, regardless of the language of the Windows operating system that you install, the IIS account name will always be IUSR, and the group name will be IIS_IUSRS.

For more information, see Understand built-in user and group accounts in IIS 7.

Attribute	Value
Well-known SID/RID	S-1-5-32-568
Type	Builtin Local
Default container	CN=Builtin, DC=<domain>, DC=
Default members	IUSR
Default member of	None
Protected by AdminSDHolder?	No
Safe to move out of default container?	
Safe to delegate management of this group to non-service admins?	
Default user rights	None

Incoming Forest Trust Builders

Members of the Incoming Forest Trust Builders group can create incoming, one-way trusts to this forest. Active Directory provides security across multiple domains or forests through domain and forest trust relationships. Before authentication can occur across trusts, Windows must determine whether the domain being requested by a user, computer, or service has a trust relationship with the logon domain of the requesting account.

To make this determination, the Windows security system computes a trust path between the domain controller for the server that receives the request and a domain controller in the domain of the requesting account. A secured channel extends to other Active Directory domains through interdomain trust relationships. This secured channel is used to obtain and verify security information, including SIDs for users and groups.

This group appears as an SID until the domain controller is made the primary domain controller and it holds the operations master (FSMO) role. This group can't be renamed, deleted, or removed.

For more information, see How domain and forest trusts work: Domain and forest trusts.

The Incoming Forest Trust Builders group applies to the Windows Server operating system in Default Active Directory security groups.

Attribute	Value
Well-known SID/RID	S-1-5-32-557
Type	Builtin Local
Default container	CN=Builtin, DC=<domain>, DC=
Default members	None
Default member of	None
Protected by AdminSDHolder?	No
Safe to move out of default container?	Can't be moved
Safe to delegate management of this group to non-service admins?	No
Default user rights	None

Key Admins

Members of this group can perform administrative actions on key objects within the domain.

The Key Admins group applies to the Windows Server operating system in Default Active Directory security groups.

Attribute	Value
Well-known SID/RID	S-1-5-21-<domain>-526
Type	Global
Default container	CN=Users, DC=<domain>, DC=
Default members	None
Default member of	None
Protected by AdminSDHolder?	Yes
Safe to move out of default container?	Yes
Safe to delegate management of this group to non-service admins?	No
Default user rights	None

Network Configuration Operators

Members of the Network Configuration Operators group can have the following administrative privileges to manage configuration of networking features:

- Modify the Transmission Control Protocol/Internet Protocol (TCP/IP) properties for a local area network (LAN) connection, which includes the IP address, the subnet mask, the default gateway, and the name servers.
- Rename the LAN connections or remote access connections that are available to all the users.
- Enable or disable a LAN connection.
- Modify the properties of all remote access connections of users.
- Delete all the remote access connections of users.
- Rename all the remote access connections of users.
- Issue `ipconfig`, `ipconfig /release`, and `ipconfig /renew` commands.
- Enter the PIN unblock key (PUK) for mobile broadband devices that support a SIM card.

This group appears as an SID until the domain controller is made the primary domain controller and it holds the operations master (FSMO) role. This group can't be renamed, deleted, or removed.

The Network Configuration Operators group applies to the Windows Server operating system in Default Active Directory security groups.

Attribute	Value
Well-known SID/RID	S-1-5-32-556
Type	Builtin Local
Default container	CN=Builtin, DC=<domain>, DC=
Default members	None
Default member of	None
Protected by AdminSDHolder?	No
Safe to move out of default container?	Can't be moved
Safe to delegate management of this group to non-service admins?	Yes
Default user rights	None

Performance Log Users

Members of the Performance Log Users group can manage performance counters, logs, and alerts locally on the server and from remote clients without being a member of the Administrators group. Specifically, members of this security group:

security group:

- Can use all the features that are available to the Performance Monitor Users group.
- Can create and modify Data Collector Sets after the group is assigned the Log on as a batch job user right.

  > ⚠ **Warning**
  >
  > If you're a member of the Performance Log Users group, you must configure Data Collector Sets that you create to run under your credentials.

  > ⓘ **Note**
  >
  > In Windows Server 2016 and later, a member of the Performance Log Users group can't create Data Collector Sets. If a member of the Performance Log Users group tries to create Data Collector Sets, they can't complete the action because access is denied.

- Can't use the Windows Kernel Trace event provider in Data Collector Sets.

For members of the Performance Log Users group to initiate data logging or modify Data Collector Sets, the group must first be assigned the Log on as a batch job user right. To assign this user right, use the Local Security Policy snap-in in Microsoft Management Console (MMC).

This group appears as an SID until the domain controller is made the primary domain controller and it holds the operations master (FSMO) role. This account can't be renamed, deleted, or moved.

The Performance Log Users group applies to the Windows Server operating system in Default Active Directory security groups.

Attribute	Value
Well-known SID/RID	S-1-5-32-559
Type	Builtin Local
Default container	CN=Builtin, DC=<domain>, DC=
Default members	None
Default member of	None
Protected by AdminSDHolder?	No
Safe to move out of default container?	Can't be moved
Safe to delegate management of this group to non-service admins?	Yes

Default user rights	Log on as a batch job: SeBatchLogonRight

Performance Monitor Users

Members of this group can monitor performance counters on domain controllers in the domain, locally and from remote clients, without being a member of the Administrators or Performance Log Users groups. The Windows Performance Monitor is an MMC snap-in that provides tools for analyzing system performance. From a single console, you can monitor application and hardware performance, customize what data you want to collect in logs, define thresholds for alerts and automatic actions, generate reports, and view past performance data in various ways.

Specifically, members of this security group:

- Can use all the features that are available to the Users group.
- Can view real-time performance data in Performance Monitor.
- Can change the Performance Monitor display properties while viewing data.
- Can't create or modify Data Collector Sets.

> ⚠ **Warning**
>
> Members of the Performance Monitor Users group can't configure Data Collection Sets.

This group appears as an SID until the domain controller is made the primary domain controller and it holds the operations master (FSMO) role. This group can't be renamed, deleted, or removed.

The Performance Monitor Users group applies to the Windows Server operating system in Default Active Directory security groups.

Attribute	Value
Well-known SID/RID	S-1-5-32-558
Type	Builtin Local
Default container	CN=Builtin, DC=<domain>, DC=
Default members	None
Default member of	None
Protected by AdminSDHolder?	No

Safe to move out of default container?	Can't be moved
Safe to delegate management of this group to non-service admins?	Yes
Default user rights	None

Pre–Windows 2000 Compatible Access

Members of the Pre–Windows 2000 Compatible Access group have Read access for all users and groups in the domain. This group is provided for backward compatibility for computers running Windows NT 4.0 and earlier. By default, the special identity group Everyone is a member of this group. Add users to this group only if they're running Windows NT 4.0 or earlier.

> ⚠ **Warning**
>
> This group appears as an SID until the domain controller is made the primary domain controller and it holds the operations master (FSMO) role.

The Pre–Windows 2000 Compatible Access group applies to the Windows Server operating system in Default Active Directory security groups.

Attribute	Value
Well-known SID/RID	S-1-5-32-554
Type	Builtin Local
Default container	CN=Builtin, DC=<domain>, DC=
Default members	If you choose the Pre–Windows 2000 Compatible Permissions mode, Everyone and Anonymous are members. If you choose the Windows 2000-only permissions mode, Authenticated Users are members.
Default member of	None
Protected by AdminSDHolder?	No
Safe to move out of default container?	Can't be moved
Safe to delegate management of this group to non-service admins?	No
Default user rights	Access this computer from the network: SeNetworkLogonRight Bypass traverse checking: SeChangeNotifyPrivilege

Print Operators

Members of this group can manage, create, share, and delete printers that are connected to domain controllers in the domain. They also can manage Active Directory printer objects in the domain. Members of this group can locally sign in to and shut down domain controllers in the domain.

This group has no default members. Because members of this group can load and unload device drivers on all domain controllers in the domain, add users with caution. This group can't be renamed, deleted, or removed.

The Print Operators group applies to the Windows Server operating system in Default Active Directory security groups.

For more information, see Assign delegated print administrator and printer permission settings in Windows Server 2012.

Attribute	Value
Well-known SID/RID	S-1-5-32-550
Type	Builtin Local
Default container	CN=Builtin, DC=<domain>, DC=
Default members	None
Default member of	None
Protected by AdminSDHolder?	Yes
Safe to move out of default container?	Can't be moved
Safe to delegate management of this group to non-service admins?	No
Default user rights	Allow log on locally: SeInteractiveLogonRight Load and unload device drivers: SeLoadDriverPrivilege Shut down the system: SeShutdownPrivilege

Protected Users

Members of the Protected Users group have extra protection against the compromise of credentials during authentication processes.

This security group is designed as part of a strategy to effectively protect and manage credentials within the enterprise. Members of this group automatically have non-configurable protection applied to their accounts. Membership in the Protected Users group is meant to be restrictive and proactively secure by default. The only way you can modify the protection for an account is to

remove the account from the security group.

This domain-related, Global group triggers non-configurable protection on devices and host computers, starting with the Windows Server 2012 R2 and Windows 8.1 operating systems. It also triggers non-configurable protection on domain controllers in domains that have a primary domain controller running Windows Server 2016 or Windows Server 2012 R2. This protection greatly reduces the memory footprint of credentials when users sign in to computers on the network from a non-compromised computer.

Depending on the account's domain functional level, members of the Protected Users group are further protected due to behavior changes in the authentication methods that are supported in Windows:

- Members of the Protected Users group can't authenticate by using the following Security Support Providers (SSPs): NTLM, Digest Authentication, or CredSSP. Passwords aren't cached on a device running Windows 10 or Windows 8.1, so the device fails to authenticate to a domain when the account is a member of the Protected User group.
- The Kerberos protocol won't use the weaker DES or RC4 encryption types in the preauthentication process. The domain must be configured to support at least the AES cipher suite.
- The user's account can't be delegated with Kerberos constrained or unconstrained delegation. If the user is a member of the Protected Users group, earlier connections to other systems might fail.
- You can change the default Kerberos ticket-granting tickets (TGTs) lifetime setting of four hours by using Authentication Policies and Silos in the Active Directory Administrative Center. In the default setting, when four hours have passed, the user must authenticate again.

The Protected Users group applies to the Windows Server operating system in Default Active Directory security groups.

This group was introduced in Windows Server 2012 R2. For more information about how this group works, see Protected Users security group.

The following table specifies the properties of the Protected Users group:

Attribute	Value
Well-known SID/RID	S-1-5-21-<domain>-525
Type	Global
Default container	CN=Users, DC=<domain>, DC=
Default members	None
Default member of	None

IPR2025-01086
Orca Security EX1021 Page 35

Protected by AdminSDHolder?	No
Safe to move out of default container?	Yes
Safe to delegate management of this group to non-service admins?	No
Default user rights	None

RAS and IAS Servers

Computers that are members of the RAS and IAS Servers group, when properly configured, can use remote access services. By default, this group has no members. Computers that are running the Routing and Remote Access Service (RRAS) and remote access services like Internet Authentication Service (IAS) and Network Policy Servers are added to the group automatically. Members of this group have access to certain properties of User objects, such as Read Account Restrictions, Read Logon Information, and Read Remote Access Information.

The RAS and IAS Servers group applies to the Windows Server operating system in Default Active Directory security groups.

Attribute	**Value**
Well-known SID/RID	S-1-5-21-<domain>-553
Type	Builtin Local
Default container	CN=Users, DC=<domain>, DC=
Default members	None
Default member of	None
Protected by AdminSDHolder?	No
Safe to move out of default container?	Yes
Safe to delegate management of this group to non-service admins?	Yes
Default user rights	None

RDS Endpoint Servers

Servers that are members in the RDS Endpoint Servers group can run virtual machines and host sessions where user RemoteApp programs and personal virtual desktops run. You must populate this group on servers running RD Connection Broker. Session Host servers and RD Virtualization Host servers used in the deployment must be in this group.

For information about Remote Desktop Services (RDS), see Host desktops and

apps in Remote Desktop Services.

Attribute	Value
Well-known SID/RID	S-1-5-32-576
Type	Builtin Local
Default container	CN=Builtin, DC=<domain>, DC=
Default members	None
Default member of	None
Protected by AdminSDHolder?	No
Safe to move out of default container?	Can't be moved
Safe to delegate management of this group to non-service admins?	
Default user rights	None

RDS Management Servers

You can use servers that are members of the RDS Management Servers group to complete routine administrative actions on servers running RDS. You must populate this group on all servers in an RDS deployment. The servers running the RDS Central Management service must be included in this group.

Attribute	Value
Well-known SID/RID	S-1-5-32-577
Type	Builtin Local
Default container	CN=Builtin, DC=<domain>, DC=
Default members	None
Default member of	None
Protected by AdminSDHolder?	No
Safe to move out of default container?	Can't be moved
Safe to delegate management of this group to non-service admins?	
Default user rights	None

RDS Remote Access Servers

Servers in the RDS Remote Access Servers group provide users with access to

RemoteApp programs and personal virtual desktops. In internet-facing deployments, these servers typically are deployed in an edge network. You must populate this group on servers running RD Connection Broker. RD Gateway servers and RD Web Access servers that are used in the deployment must be in this group.

For more information, see Host desktops and apps in Remote Desktop Services.

Attribute	Value
Well-known SID/RID	S-1-5-32-575
Type	Builtin Local
Default container	CN=Builtin, DC=<domain>, DC=
Default members	None
Default member of	None
Protected by AdminSDHolder?	No
Safe to move out of default container?	Can't be moved
Safe to delegate management of this group to non-service admins?	
Default user rights	None

Read-only Domain Controllers

This group is composed of the RODCs in the domain. An RODC makes it possible for organizations to easily deploy a domain controller in scenarios in which physical security can't be guaranteed, such as in branch office locations or when local storage of all domain passwords is considered a primary threat, like in an extranet or application-facing role.

Because you can delegate administration of an RODC to a domain user or security group, an RODC is well suited for a site that shouldn't have a user who is a member of the Domain Admins group. An RODC has the following functionality:

- Contains read-only AD DS database
- Unidirectional replication
- Credential caching
- Administrator role separation
- Contains read-only Domain Name System (DNS)

For more information, see Understand planning and deployment for read-only

domain controllers.

Attribute	Value
Well-known SID/RID	S-1-5-21-<domain>-521
Type	Global
Default container	CN=Users, DC=<domain>, DC=
Default members	None
Default member of	Denied RODC Password Replication
Protected by AdminSDHolder?	Yes
Safe to move out of default container?	Yes
Safe to delegate management of this group to non-service admins?	
Default user rights	See Denied RODC Password Replication

Remote Desktop Users

Use the Remote Desktop Users group on an RD Session Host server to grant users and groups permissions to remotely connect to an RD Session Host server. This group can't be renamed, deleted, or removed. The group appears as an SID until the domain controller is made the primary domain controller and it holds the operations master (FSMO) role.

The Remote Desktop Users group applies to the Windows Server operating system in Default Active Directory security groups.

Attribute	Value
Well-known SID/RID	S-1-5-32-555
Type	Builtin Local
Default container	CN=Builtin, DC=<domain>, DC=
Default members	None
Default member of	None
Protected by AdminSDHolder?	No
Safe to move out of default container?	Can't be moved
Safe to delegate management of this group to non-service admins?	Yes
Default user rights	None

Remote Management Users

Members of the Remote Management Users group can access Windows Management Instrumentation (WMI) resources over management protocols like WS-Management via the Windows Remote Management service. Access to WMI resources applies only to WMI namespaces that grant access to the user.

Use the Remote Management Users group to allow users to manage servers through the Server Manager console. Use the WinRMRemoteWMIUsers_ group to allow users to remotely run Windows PowerShell commands.

For more information, see What's new in MI? and About WMI.

Attribute	Value
Well-known SID/RID	S-1-5-32-580
Type	Builtin Local
Default container	CN=Builtin, DC=<domain>, DC=
Default members	None
Default member of	None
Protected by AdminSDHolder?	No
Safe to move out of default container?	Can't be moved
Safe to delegate management of this group to non-service admins?	
Default user rights	None

Replicator

Computers that are members of the Replicator group support file replication in a domain. Windows Server operating systems use the File Replication Service (FRS) to replicate system policies and logon scripts that are stored in the System Volume folder (sysvol folder). Each domain controller keeps a copy of the sysvol folder for network clients to access. FRS can also replicate data for the Distributed File System (DFS) and sync the content of each member in a replica set as defined by DFS. FRS can copy and maintain shared files and folders on multiple servers simultaneously. When changes occur, content is synced immediately within sites and on a schedule between sites.

> ⚠ **Warning**
>
> In Windows Server 2008 R2, you can't use FRS to replicate DFS folders or custom (non-sysvol) data. A Windows Server 2008 R2 domain controller

can still use FRS to replicate the contents of sysvol folder shared resource in a domain that uses FRS to replicate the sysvol folder shared resource between domain controllers. However, Windows Server 2008 R2 servers can't use FRS to replicate the contents of any replica set except the sysvol folder shared resource. The DFS Replication service is a replacement for FRS. You can use DFS Replication to replicate the contents of a sysvol folder shared resource, DFS folders, and other custom (non-sysvol) data. You should migrate all non-sysvol FRS replica sets to DFS Replication.

For more information, see:

- File Replication Service (FRS) is deprecated in Windows Server 2008 R2 (Windows)
- DFS namespaces and DFS Replication overview

Attribute	Value
Well-known SID/RID	S-1-5-32-552
Type	Builtin Local
Default container	CN=Builtin, DC=<domain>, DC=
Default members	None
Default member of	None
Protected by AdminSDHolder?	Yes
Safe to move out of default container?	Can't be moved
Safe to delegate management of this group to non-service admins?	
Default user rights	None

Schema Admins

Members of the Schema Admins group can modify the Active Directory schema. This group exists only in the root domain of an Active Directory forest of domains. This group is a Universal group if the domain is in native mode. This group is a Global group if the domain is in mixed mode.

The group is authorized to make schema changes in Active Directory. By default, the only member of the group is the Administrator account for the forest root domain. This group has full administrative access to the schema.

Any of the service administrator groups in the root domain can modify the membership of this group. This group is considered a service administrator account because its members can modify the schema, which governs the structure and content of the entire directory.

For more information, see What is the Active Directory schema?

The Schema Admins group applies to the Windows Server operating system in Default Active Directory security groups.

Attribute	Value
Well-known SID/RID	S-1-5-21-<root domain>-518
Type	Universal (if Domain is in Native-Mode) else Global
Default container	CN=Users, DC=<domain>, DC=
Default members	Administrator
Default member of	Denied RODC Password Replication
Protected by AdminSDHolder?	Yes
Safe to move out of default container?	Yes
Safe to delegate management of this group to non-service admins?	No
Default user rights	See Denied RODC Password Replication

Server Operators

Members of the Server Operators group can administer domain controllers. This group exists only on domain controllers. By default, the group has no members. Members of the Server Operators group can take the following actions: sign in to a server interactively, create and delete network shared resources, start and stop services, back up and restore files, format the hard disk drive of the computer, and shut down the computer. This group can't be renamed, deleted, or removed.

By default, this built-in group has no members. The group has access to server configuration options on domain controllers. Its membership is controlled by the service administrator groups Administrators and Domain Admins in the domain, and by the Enterprise Admins group in the forest root domain. Members in this group can't change any administrative group memberships. This group is considered a service administrator account because its members have physical access to domain controllers. Members of this group can perform maintenance tasks like backup and restore, and they can change binaries that are installed on the domain controllers. See the group's default user rights in the following table.

The Server Operators group applies to the Windows Server operating system in Default Active Directory security groups.

Attribute	Value

Well-known SID/RID	S-1-5-32-549
Type	Builtin Local
Default container	CN=Builtin, DC=<domain>, DC=
Default members	None
Default member of	None
Protected by AdminSDHolder?	Yes
Safe to move out of default container?	Can't be moved
Safe to delegate management of this group to non-service admins?	No
Default user rights	Allow log on locally: SeInteractiveLogonRight Back up files and directories: SeBackupPrivilege Change the system time: SeSystemTimePrivilege Change the time zone: SeTimeZonePrivilege Force shutdown from a remote system: SeRemoteShutdownPrivilege Restore files and directories: Restore files and directories SeRestorePrivilege Shut down the system: SeShutdownPrivilege

Storage Replica Administrators

Members of the Storage Replica Administrators group have complete and unrestricted access to all features of Storage Replica. The Storage Replica Administrators group applies to the Windows Server operating system in Default Active Directory security groups.

Attribute	**Value**
Well-known SID/RID	S-1-5-32-582
Type	Builtin Local
Default container	CN=Builtin, DC=<domain>, DC=
Default members	None
Default member of	None
Protected by AdminSDHolder?	No
Safe to move out of default container?	Yes

Safe to delegate management of this group to non-service admins?	No
Default user rights	None

System Managed Accounts

Membership of the System Managed Accounts group is managed by the system.

The System Managed Accounts group applies to the Windows Server operating system in Default Active Directory security groups.

Attribute	Value
Well-known SID/RID	S-1-5-32-581
Type	Builtin Local
Default container	CN=Builtin, DC=<domain>, DC=
Default members	Users
Default member of	None
Protected by AdminSDHolder?	No
Safe to move out of default container?	Yes
Safe to delegate management of this group to non-service admins?	No
Default user rights	None

Terminal Server License Servers

Members of the Terminal Server License Servers group can update user accounts in Active Directory with information about license issuance. The group is used to track and report TS Per User CAL usage. A TS Per User CAL gives one user the right to access an instance of Terminal Server from an unlimited number of client computers or devices. This group appears as an SID until the domain controller is made the primary domain controller and it holds the operations master (FSMO) role. This group can't be renamed, deleted, or removed.

For more information about this security group, see Terminal Services License Server security group configuration.

The Terminal Server License Servers group applies to the Windows Server operating system in Default Active Directory security groups.

Attribute	Value
Well-known SID/RID	S-1-5-32-561
Type	Builtin Local
Default container	CN=Builtin, DC=<domain>, DC=
Default members	None
Default member of	None
Safe to move out of default container?	Can't be moved
Protected by AdminSDHolder?	No
Safe to delegate management of this group to non-service admins?	Yes
Default user rights	None

Users

Members of the Users group are prevented from making accidental or intentional system-wide changes. Members of this group can run most applications. After the initial installation of the operating system, the only member is the Authenticated Users group. When a computer joins a domain, the Domain Users group is added to the Users group on the computer.

Users can do tasks like run an application, use local and network printers, shut down the computer, and lock the computer. Users can install applications that only they can use if the installation program of the application supports per-user installation. This group can't be renamed, deleted, or removed.

The Users group applies to the Windows Server operating system in Default Active Directory security groups.

This security group includes the following changes since Windows Server 2008:

- In Windows Server 2008 R2, Interactive was added to the default members list.
- In Windows Server 2012, the default Member Of list changed from Domain Users to none.

Attribute	Value
Well-known SID/RID	S-1-5-32-545
Type	Builtin Local
Default container	CN=Builtin, DC=<domain>, DC=
Default members	Authenticated Users

IPR2025-01086
Orca Security EX1021 Page 45

	Domain Users Interactive
Default member of	None
Protected by AdminSDHolder?	No
Safe to move out of default container?	Can't be moved
Safe to delegate management of this group to non-service admins?	No
Default user rights	None

Windows Authorization Access

Members of this group have access to the computed token GroupsGlobalAndUniversal attribute on User objects. Some applications have features that read the token-groups-global-and-universal (TGGAU) attribute on user account objects or on computer account objects in AD DS. Some Win32 functions make it easier to read the TGGAU attribute. Applications that read this attribute or that call an API (a *function*) that reads this attribute don't succeed if the calling security context doesn't have access to the attribute. This group appears as an SID until the domain controller is made the primary domain controller and it holds the operations master (FSMO) role. This group can't be renamed, deleted, or removed.

The Windows Authorization Access group applies to the Windows Server operating system in Default Active Directory security groups.

Attribute	**Value**
Well-known SID/RID	S-1-5-32-560
Type	Builtin Local
Default container	CN=Builtin, DC=<domain>, DC=
Default members	Enterprise Domain Controllers
Default member of	None
Protected by AdminSDHolder?	No
Safe to move out of default container?	Can't be moved
Safe to delegate management of this group to non-service admins?	Yes
Default user rights	None

WinRMRemoteWMIUsers_

In Windows Server 2012 and Windows 8, a **Share** tab was added to the Advanced Security Settings user interface. This tab displays the security properties of a remote file share. To view this information, you must have the following permissions and memberships, as appropriate for the version of Windows Server that the file server is running.

The WinRMRemoteWMIUsers_ group applies to the Windows Server operating system in Default Active Directory security groups.

- If the file share is hosted on a server that's running a supported version of the operating system:
  - You must be a member of the WinRMRemoteWMIUsers__ group or the BUILTIN\Administrators group.
  - You must have Read permissions to the file share.
- If the file share is hosted on a server that's running a version of Windows Server that's earlier than Windows Server 2012:
  - You must be a member of the BUILTIN\Administrators group.
  - You must have Read permissions to the file share.

In Windows Server 2012, the Access Denied Assistance functionality adds the Authenticated Users group to the local WinRMRemoteWMIUsers__ group. When the Access Denied Assistance functionality is enabled, all authenticated users who have Read permissions to the file share can view the file share permissions.

> **Note**
>
> The WinRMRemoteWMIUsers__ group allows running Windows PowerShell commands remotely. In contrast, you typically use the **Remote Management Users** group to allow users to manage servers by using the Server Manager console.

Attribute	Value
Well-known SID/RID	S-1-5-21-<domain>-<variable RI>
Type	Domain local
Default container	CN=Users, DC=<domain>, DC=
Default members	None
Default member of	None

Protected by AdminSDHolder?	No
Safe to move out of default container?	Yes
Safe to delegate management of this group to non-service admins?	
Default user rights	None

See also

- Security principals
- Special identity groups
- Access control overview

Feedback

Submit and view feedback for

This product | This page

View all page feedback

English (United States) Theme

Manage cookies Previous Versions Blog Contribute Privacy Terms of Use Trademarks © Microsoft 2023