Network access Do not allow anonymous enumeration - Windows 10

By vinaypamnani-msft

Archived: 2026-04-05 16:25:34 UTC

Applies to

- Windows 10

Describes the best practices, location, values, and security considerations for the **Network access: Do not allow anonymous enumeration of SAM accounts and shares** security policy setting.

Reference

This policy setting determines which other permissions will be assigned for anonymous connections to the device. Windows allows anonymous users to perform certain activities, such as enumerating the names of domain accounts and network shares. This permission is convenient, for example, when an administrator wants to give access to users in a trusted domain that doesn't maintain a reciprocal trust. However, even with this policy setting enabled, anonymous users will have access to resources with permissions that explicitly include the built-in group, ANONYMOUS LOGON.

This policy setting has no impact on domain controllers. Misuse of this policy setting is a common error that can cause data loss or problems with data access or security.

Possible values

- Enabled
- Disabled

  No other permissions can be assigned by the administrator for anonymous connections to the device. Anonymous connections will rely on default permissions. However, an unauthorized user could anonymously list account names and use the information to attempt to guess passwords or perform social-engineering attacks.

- Not defined

Location

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

Default values

The following table lists the actual and effective default values for this policy. Default values are also listed on the policy's property page.

Server type or GPO	Default value
Default Domain Policy	Not defined
Default Domain Controller Policy	Not defined
Stand-Alone Server Default Settings	Disabled
DC Effective Default Settings	Disabled
Member Server Effective Default Settings	Disabled
Client Computer Effective Default Settings	Disabled

Policy management

This section describes features and tools that are available to help you manage this policy.

Restart requirement

None. Changes to this policy become effective without a device restart when they're saved locally or distributed through Group Policy.

Policy conflicts

Even with this policy setting enabled, anonymous users will have access to resources with permissions that explicitly include the built-in group, ANONYMOUS LOGON (on systems earlier than Windows Server 2008 and Windows Vista).

Group Policy

This policy has no impact on domain controllers.

Security considerations

This section describes how an attacker might exploit a feature or its configuration, how to implement the countermeasure, and the possible negative consequences of countermeasure implementation.

Vulnerability

An unauthorized user could anonymously list account names and shared resources and use the information to attempt to guess passwords or perform social-engineering attacks.

Countermeasure

Enable the **Network access: Do not allow anonymous enumeration of SAM accounts and shares** setting.

Potential impact

It's impossible to grant access to users of another domain across a one-way trust because administrators in the trusting domain are unable to enumerate lists of accounts in the other domain. Users who access file and print servers anonymously are unable to list the shared network resources on those servers; the users must be authenticated before they can view the lists of shared folders and printers.

- Security Options
