Netdom trust

By robinharwood

Archived: 2026-04-06 15:47:46 UTC

The `netdom trust` command allows administrators to manage, establish, verify, or reset trust relationships between domains. It's available if you have the Active Directory Domain Services (AD DS) server role installed. It's also available if you install the AD DS tools that are part of the Remote Server Administration Tools (RSAT). For more information, see How to Administer Microsoft Windows Client and Server Computers Locally and Remotely.

To use `netdom trust`, you must run the command from an elevated command prompt.

Note

The `netdom trust` command can't be used to create a forest trust between two AD DS forests. To create a cross-forest trust between two AD DS forests, use the **Active Directory Domains and Trusts** snap-in to create and manage forest trusts. Scripting solution such as using PowerShell is also an option for managing these types of trusts if you need to automate the process.

```
netdom trust trusting_domain_name /Domain:trusted_domain_name [/UserD:user]
            [/PasswordD:[password | *]] [/UserO:user] [/PasswordO:[password | *]]
            [/Verify] [/Reset] [/PasswordT:new_realm_trust_password]
            [/Add] [/Remove] [/Twoway] [/Realm] [/Kerberos]
            [/Transitive[:{yes | no}]]
            [/OneSide:{trusted | trusting}] [/Force] [/Quarantine[:{yes | no}]]
            [/NameSuffixes:trust_name [/ToggleSuffix:#]]
            [/EnableSIDHistory[:{yes | no}]] [/ForestTransitive[:{yes | no}]]
            [/CrossOrganization[:{yes | no}]] [/AddTLN:TopLevelName]
            [/AddTLNEX:TopLevelNameExclusion] [/RemoveTLN:TopLevelName]
            [/RemoveTLNEX:TopLevelNameExclusion] [/SecurePasswordPrompt]
            [/EnableTgtDelegation[:{yes | no}]] [/EnablePIMTrust[:{yes | no}]]
            [/AuthTargetValidation[:{yes | no}]] [/ChildDomain:childdomainname]
            [/InvokeTrustScanner]
```

Parameter	Description
`<TrustingDomainName>`	Specifies the name of the trusting domain.
`/domain:` `<TrustedDomainName>`	Specifies the name of the trusted domain or non-Windows realm. If not specified, the current domain to which the current computer belongs is used.

Parameter	Description
`/userd:<User>`	Specifies the user account to use for the connection with the domain specified using the `/domain` parameter. Defaults to the current user account if not specified.
`/passwordd:<Password>` | `*`	Specifies the password for the user account used with `/userd`. Use `*` to prompt for the password.
`/usero:<User>`	Specifies the user account to use for the connection with the trusting domain. Defaults to the current user account if not specified.
`/passwordo:<Password>` | `*`	Specifies the password for the user account used with `/usero`. Use `*` to prompt for the password.
`/verify`	Verifies the secure channel secrets for a specific trust relationship.
`/reset`	Resets the trust secret between trusted domains or between the domain controller (DC) and the workstation.
`/passwordt:<NewRealmTrustPassword>`	Sets a new trust password. This option is valid only with the `/add` or `/reset` parameters, and only if one of the specified domains is a non-Windows Kerberos realm. The trust password is configured on the Windows domain only, so credentials for the non-Windows domain aren't required.
`/add`	Creates a trust.
`/remove`	Removes a trust.
`/twoway`	Establishes a two-way trust relationship.
`/realm`	Creates the trust for a non-Windows Kerberos realm. Valid only with the `/add` parameter. The `/passwordt` parameter is required.
`/kerberos`	Uses the Kerberos protocol to verify authentication between a workstation and the specified domain. Requires credentials for both the source and target domains.
`/transitive:Yes` | `No`	Applies only to non-Windows Kerberos realm trusts. Use `yes` to make the trust transitive, or `no` to make it non-transitive. If not specified, displays the current transitivity setting.
`/oneside:trusted` | `trusting`	Specifies that the trust operation should be conducted on only one side of the trust relationship. Use `trusted` to apply the operation to the domain specified with the `/domain` parameter (the "trusted" domain), or use `trusting` to apply it to the "trusting" domain. This option is only valid

Parameter	Description
	with the `/add` and `/remove` parameters. When used with `/add`, the `/passwordt` parameter is also required. - **Trusted Domain**: This is the domain that is being trusted. In a trust relationship, the trusting domain allows users from the trusted domain to access its resources. The trusted domain's users are given certain permissions or access within the trusting domain. - **Trusting Domain**: This is the domain that trusts another domain (the trusted domain). It essentially means that the trusting domain is extending its trust to the users of the trusted domain, allowing them to access resources within the trusting domain.
`/force`	Removes both the trusted domain object and cross-reference object from the forest. The full DNS name must be specified for the domain. Valid with the `/remove` parameter and if specified, a child domain is removed.
`/quarantine:Yes` | `No`	Sets or clears the domain quarantine attribute. If not specified, displays the current state. `Yes` accepts only SIDs from the directly trusted domain. `No` accepts any SID (default). Specifying `/quarantine` without an option displays the current state.
`/namesuffixes:<TrustName>`	Lists the routed name suffixes for the specified trust. This parameter is valid only for a forest trust or a forest transitive non-Windows realm trust. Use `/usero` and `/passwordo` for authentication if needed. The `/domain` parameter isn't required for this operation.
`/togglesuffix:#`	Use this parameter with `/namesuffixes` to enable or disable a specific name suffix. Specify the number of the name entry as shown in the output of the preceding `/namesuffixes` command. You can't change the status of names that are in conflict until the conflicting name in the other trust is disabled. Always run `/namesuffixes` immediately before `/togglesuffix` because the order of name entries might change.
`/enablesidhistory:Yes` | `No`	Enables (`Yes`) or disables (`No`) migrated users in the trusted forest to use SID history to access resources. Valid only for outbound forest trusts. Only enable if you trust the administrators of the trusted forest. If an option isn't specified, the current state is displayed.
`/foresttransitive:Yes` | `No`	Marks the trust as forest transitive (yes) or not (no). Valid only for AD trusts and non-Windows realm trusts only on the root domain for a forest. If not specified, displays the current state.

Parameter	Description
`/selectiveauth:Yes` | `No`	Enables (`Yes`) or disables (`No`) selective authentication across the trust. Valid only on outbound forest and external trusts. If not specified, displays the current state.
`/addtln:<TopLevelName>`	Adds the specified top-level DNS name suffix to the forest trust info for the trust. Valid only for a forest transitive non-Windows realm trust and only on the root domain for a forest. Run `/namesuffixes` for a list of name suffixes.
`/addtlnex:<TopLevelNameExclusion>`	Adds the specified top-level name exclusion (DNS name suffix) to the forest trust info for the trust. Valid only for a forest transitive non-Windows realm trust and only on the root domain for a forest. Run `/namesuffixes` for a list of name suffixes.
`/removetln:<TopLevelName>`	Removes the specified top-level DNS name suffix from the forest trust info for the trust. Valid only for a forest transitive non-Windows realm trust and only on the root domain for a forest. Run `/namesuffixes` for a list of name suffixes.
`/removetlnex:<TopLevelNameExclusion>`	Removes the specified top-level name exclusion (DNS name suffix) from the forest trust info for the trust. Valid only for a forest transitive non-Windows realm trust and only on the root domain for a forest. Run `/namesuffixes` for a list of name suffixes.
`/securepasswordprompt`	Opens a secure credentials popup for entering credentials. This is useful when specifying smartcard credentials. This option is effective only when the password is entered as `*`.
`/enabletgtdelegation:Yes` | `No`	Enables (`Yes`) or disables (`No`) Kerberos full delegation on outbound forest trusts. When set to `No` , Kerberos full delegation is blocked, preventing services in the other forest from receiving forwarded Ticket Granting Tickets (TGTs). **Disabling** this option means that services in the other forest configured for *"Trust this computer/user for delegation to any service"* isn't able to use Kerberos full delegation with any account in this forest.
`/enablepimtrust:Yes` | `No`	Enables (`Yes`) or disables (`No`) Privileged Identity Management (PIM) trust behaviors for this trust. The trust must be marked as forest transitive before enabling this attribute. If `/enablepimtrust` is specified without `Yes` or `No` , the current state of this attribute is displayed.

Parameter	Description
`/authtargetvalidation:Yes` | `No`	Enables (`Yes`) or disables (`No`) authentication target validation for authentication requests on the specified trust. For forest trusts, you can limit this setting to a specific child domain using the `/childdomain` parameter. **Disabling** this validation might expose your environment to security risks from the remote forest and should only be done when necessary.
`/childdomain:` `<ChildDomainName>`	Use to target a child domain within a larger domain structure when performing trust-related operations to ensure that the trust operation applies directly to the child domain. This parameter is useful in scenarios where precise control over trust relationships is needed within complex domain environments.
`/invoketrustscanner`	Initiates a trust scan for the specified trusting domain. If the trusting domain is set to `*` , all trusts are scanned. This command must be executed locally on the primary DC. The trust scanner typically runs automatically. Use this command only for troubleshooting or support purposes.
`help` | `/?`	Displays help at the command prompt.

To set the domain **USA-Chicago** to trust the domain **NorthAmerica**, run the following command:

```
netdom trust USA-Chicago /domain:NorthAmerica /add /userd:NorthAmerica\admin /passwordd:* /usero:USA-Chicago\ad
```

To establish a two-way trust between the **engineering.contoso.com** domain and the **marketing.contoso.com** domain, run the following command:

```
netdom trust engineering.contoso.com /domain:marketing.contoso.com /add /twoway /usero:admin@engineering.contos
```

To establish a one-way trust where the **NorthAmerica** domain trusts the non-Windows Kerberos realm **ATHENA**, run the following command:

```
netdom trust NorthAmerica /domain:ATHENA /add /passwordt:* /realm
```

Note

Verifying a specific trust relationship requires credentials unless the user has domain administrator privileges on both domains.

If you want to set the Kerberos realm **ATHENA** to trust the **NorthAmerica** domain, run the following command:

```
netdom trust NorthAmerica /domain:ATHENA /add /realm
```

To undo (remove) the trust that **USA-Chicago** has with **NorthAmerica**, run the following command:

```
netdom trust USA-Chicago /domain:NorthAmerica /remove
```

To reset the secure channel for the one-way trust between **NorthAmerica** and **USA-Chicago**, run the following command:

```
netdom trust USA-Chicago /domain:NorthAmerica /userd:NorthAmerica\admin /passwordd:* /reset
```

To verify that the trust relationship between the **MyDomain** domain and the **devgroup.example.com** domain supports Kerberos authentication, run the following command:

```
netdom trust MyDomain /domain:devgroup.example.com /verify /kerberos /userd:devgroup\admin /passwordd:* /usero
```

Note

You can't run this trust operation from a remote location. You must run the operation on the workstation that you want to test.

To enable or disable the first routed name suffix in the list generated by the previous command, run the following command:

```
netdom trust myTestDomain /domain:foresttrustpartnerdomain /namesuffixes /togglesuffix:1
```

You can only add a DNS name suffix for a trust that is a forest transitive non-Windows realm trust. The same restriction applies to the parameters for managing name suffix routing within a forest trust:

- `/addtln`
- `/addtlnex`
- `/removetln`
- `/removetlnex`

Command-Line Syntax Key
