



Kerberos Commands

This chapter describes the commands used to configure Kerberos. Kerberos is a secret-key network authentication protocol, developed at Massachusetts Institute of Technology (MIT), that uses the Data Encryption Standard (DES) cryptographic algorithm for encryption and authentication. Kerberos was designed to authenticate requests for network resources. Kerberos, like other secret-key systems, is based on the concept of a trusted third party that performs secure verification of users and services. In the Kerberos protocol, this trusted third party is called the key distribution center (KDC).

For information on how to configure Kerberos, refer to the “Configuring Kerberos” chapter in the *Security Configuration Guide*. For configuration examples using the commands in this chapter, refer to the “Kerberos Configuration Examples” section located at the end of the “Configuring Kerberos” chapter in the *Security Configuration Guide*.

clear kerberos creds

To delete the contents of the credentials cache, use the **clear kerberos creds** privileged EXEC command.

clear kerberos creds

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|---------|------------------------------|
| 11.1 | This command was introduced. |

Usage Guidelines

Credentials are cleared when the user logs out.

Cisco supports Kerberos 5.

Examples

The following example illustrates the **clear kerberos creds** command:

```
cisco-2500> show kerberos creds
Default Principal: chet@cisco.com
Valid Starting      Expires              Service Principal
18-Dec-1995 16:21:07  19-Dec-1995 00:22:24  krbtgt/CISCO.COM@CISCO.COM

cisco-2500> clear kerberos creds
cisco-2500> show kerberos creds
No Kerberos credentials.

cisco-2500>
```

Related Commands

| Command | Description |
|----------------------------|--|
| show kerberos creds | Displays the contents of your credentials cache. |

kerberos clients mandatory

To cause the **rsh**, **rcp**, **rlogin**, and **telnet** commands to fail if they cannot negotiate the Kerberos protocol with the remote server, use the **kerberos clients mandatory** global configuration command. Use the **no** form of this command to make Kerberos optional.

kerberos clients mandatory

no kerberos clients mandatory

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

| Release | Modification |
|---------|------------------------------|
| 11.2 | This command was introduced. |

Usage Guidelines

If this command is not configured and the user has Kerberos credentials stored locally, the **rsh**, **rcp**, **rlogin**, and **telnet** commands attempt to negotiate the Kerberos protocol with the remote server and will use the non-Kerberized protocols if unsuccessful.

If this command is not configured and the user has no Kerberos credentials, the standard protocols for **rcp** and **rsh** are used to negotiate the Kerberos protocol.

Examples

The following example causes the **rsh**, **rcp**, **rlogin**, and **telnet** commands to fail if they cannot negotiate the Kerberos protocol with the remote server:

```
kerberos clients mandatory
```

Related Commands

| Command | Description |
|-------------------------------------|--|
| connect | Logs in to a host that supports Telnet, rlogin, or LAT. |
| kerberos credentials forward | Forces all network application clients on the router to forward the Kerberos credentials of users upon successful Kerberos authentication. |
| rlogin | Logs in to a UNIX host using rlogin. |
| rsh | Executes a command remotely on a remote rsh host. |
| telnet | Logs in to a host that supports Telnet. |

kerberos credentials forward

To force all network application clients on the router to forward users' Kerberos credentials upon successful Kerberos authentication, use the **kerberos credentials forward** global configuration command. Use the **no** form of this command to turn off Kerberos credentials forwarding.

kerberos credentials forward

no kerberos credentials forward

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

| Release | Modification |
|---------|------------------------------|
| 11.2 | This command was introduced. |

Usage Guidelines

Enable credentials forwarding to have users' TGTs forwarded to the host on which they authenticate. In this way, users can connect to multiple hosts in the Kerberos realm without running the KINIT program each time they need to get a TGT.

Examples

The following example forces all network application clients on the router to forward users' Kerberos credentials upon successful Kerberos authentication:

```
kerberos credentials forward
```

Related Commands

| Command | Description |
|----------------|---|
| connect | Logs in to a host that supports Telnet, rlogin, or LAT. |
| rlogin | Logs in to a UNIX host using rlogin. |
| rsh | Executes a command remotely on a remote rsh host. |
| telnet | Logs in to a host that supports Telnet. |

kerberos instance map

To map Kerberos instances to Cisco IOS privilege levels, use the **kerberos instance map** global configuration command. Use the **no** form of this command to remove a Kerberos instance map.

kerberos instance map *instance privilege-level*

no kerberos instance map *instance*

| | | |
|---------------------------|---|--|
| Syntax Description | <i>instance</i> | Name of a Kerberos instance. |
| | <i>privilege-level</i> | The privilege level at which a user is set if the user's Kerberos principal contains the matching Kerberos instance. You can specify up to 16 privilege levels, using numbers 0 through 15. Level 1 is normal EXEC-mode user privileges. |
| Defaults | Privilege level 1 | |
| Command Modes | Global configuration | |
| Command History | Release | Modification |
| | 11.2 | This command was introduced. |
| Usage Guidelines | Use this command to create user instances with access to administrative commands. | |
| Examples | The following example sets the privilege level to 15 for authenticated Kerberos users with the <i>admin</i> instance in Kerberos realm: kerberos instance map admin 15 | |
| Related Commands | Command | Description |
| | aaa authorization | Sets parameters that restrict network access to a user. |

kerberos local-realm

To specify the Kerberos realm in which the router is located, use the **kerberos local-realm** global configuration command. Use the **no** form of this command to remove the specified Kerberos realm from this router.

kerberos local-realm *kerberos-realm*

no kerberos local-realm

Syntax Description

kerberos-realm The name of the default Kerberos realm. A Kerberos realm consists of users, hosts, and network services that are registered to a Kerberos server. The Kerberos realm must be in uppercase characters.

Defaults

Disabled

Command Modes

Global configuration

Command History

| Release | Modification |
|---------|------------------------------|
| 11.1 | This command was introduced. |

Usage Guidelines

The router can be located in more than one realm at a time. However, there can only be one instance of Kerberos local-realm. The realm specified with this command is the default realm.

Examples

The following example specify the Kerberos realm in which the router is located as DOMAIN.COM:

```
kerberos local-realm DOMAIN.COM
```

Related Commands

| Command | Description |
|-------------------------------|--|
| kerberos preauth | Specifies a preauthentication method to use to communicate with the KDC. |
| kerberos realm | Maps a host name or DNS domain to a Kerberos realm. |
| kerberos server | Specifies the location of the Kerberos server for a given Kerberos realm. |
| kerberos srvtab entry | Retrieves a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration. |
| kerberos srvtab remote | Retrieves a krb5 SRVTAB file from the specified host. |

kerberos preauth

To specify a preauthentication method to use to communicate with the KDC, use the **kerberos preauth** global configuration command. Use the **no** form of this command to disable Kerberos preauthentication.

```
kerberos preauth [encrypted-unix-timestamp | none]
no kerberos preauth
```

Syntax Description

encrypted-unix-timestamp (Optional) Use an encrypted UNIX timestamp as a quick authentication method when communicating with the KDC.

none (Optional) Do not use Kerberos preauthentication.

Defaults

Disabled

Command Modes

Global configuration

Command History

| Release | Modification |
|---------|------------------------------|
| 11.2 | This command was introduced. |

Usage Guidelines

It is more secure to use a preauthentication for communications with the KDC. However, communication with the KDC will fail if the KDC does not support this particular version of **kerberos preauth**. If that happens, turn off the preauthentication with the **none** option.

The **no** form of this command is equivalent to using the **none** keyword.

Examples

The following example enables Kerberos preauthentication:

```
kerberos preauth encrypted-unix-timestamp
```

The following example disables Kerberos preauthentication:

```
kerberos preauth none
```

Related Commands

| Command | Description |
|-------------------------------|--|
| kerberos local-realm | Specifies the Kerberos realm in which the router is located. |
| kerberos server | Specifies the location of the Kerberos server for a given Kerberos realm. |
| kerberos srvtab entry | Retrieves a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration. |
| kerberos srvtab remote | Retrieves a krb5 SRVTAB file from the specified host. |

kerberos realm

To map a host name or Domain Name System (DNS) domain to a Kerberos realm, use the **kerberos realm** global configuration command. Use the **no** form of this command to remove a Kerberos realm map.

```
kerberos realm {dns-domain | host} kerberos-realm
```

```
no kerberos realm {dns-domain | host} kerberos-realm
```

Syntax Description

| | |
|-----------------------|---|
| <i>dns-domain</i> | Name of a DNS domain or host. |
| <i>host</i> | Name of a DNS host. |
| <i>kerberos-realm</i> | Name of the Kerberos realm to which the specified domain or host belongs. |

Defaults

Disabled

Command Modes

Global configuration

Command History

| Release | Modification |
|---------|------------------------------|
| 11.1 | This command was introduced. |

Usage Guidelines

DNS domains are specified with a leading dot (.) character; host names cannot begin with a dot (.) character. There can be multiple entries of this line.

A Kerberos realm consists of users, hosts, and network services that are registered to a Kerberos server. The Kerberos realm must be in uppercase characters. The router can be located in more than one realm at a time. Kerberos realm names must be in all uppercase characters.

Examples

The following example maps the domain name, domain.com, to the Kerberos realm, DOMAIN.COM:

```
kerberos realm .domain.com DOMAIN.COM
```

Related Commands

| Command | Description |
|-------------------------------|--|
| kerberos local-realm | Specifies the Kerberos realm in which the router is located. |
| kerberos server | Specifies the location of the Kerberos server for a given Kerberos realm. |
| kerberos srvtab entry | Retrieves a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration. |
| kerberos srvtab remote | Retrieves a krb5 SRVTAB file from the specified host. |

kerberos server

To specify the location of the Kerberos server for a given Kerberos realm, use the **kerberos server** global configuration command. Use the **no** form of this command to remove a Kerberos server for a specified Kerberos realm.

```
kerberos server kerberos-realm {hostname | ip-address} [port-number]
```

```
no kerberos server kerberos-realm {hostname | ip-address}
```

Syntax Description

| | |
|-----------------------|--|
| <i>kerberos-realm</i> | Name of the Kerberos realm. A Kerberos realm consists of users, hosts, and network services that are registered to a Kerberos server. The Kerberos realm must be in uppercase letters. |
| <i>hostname</i> | Name of the host functioning as a Kerberos server for the specified Kerberos realm (translated into an IP address at the time of entry). |
| <i>ip-address</i> | IP address of the host functioning as a Kerberos server for the specified Kerberos realm. |
| <i>port-number</i> | (Optional) Port that the KDC/TGS monitors (defaults to 88). |

Defaults

Disabled

Command Modes

Global configuration

Command History

| Release | Modification |
|---------|------------------------------|
| 11.1 | This command was introduced. |

Usage Guidelines

None.

Examples

The following example specifies 192.168.47.66 as the Kerberos server for the Kerberos realm DOMAIN.COM:

```
kerberos server DOMAIN.COM 192.168.47.66
```

Related Commands

| Command | Description |
|-------------------------------|--|
| kerberos local-realm | Specifies the Kerberos realm in which the router is located. |
| kerberos realm | Maps a host name or DNS domain to a Kerberos realm. |
| kerberos srvtab entry | Retrieves a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration. |
| kerberos srvtab remote | Retrieves a krb5 SRVTAB file from the specified host. |

kerberos srvtab entry

To retrieve a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration, use the **kerberos srvtab remote** global configuration command (not **kerberos srvtab entry**). (The Kerberos SRVTAB entry is the router's locally stored SRVTAB.) Use the **no** form of this command to remove a SRVTAB entry from the router's configuration.

kerberos srvtab entry *kerberos-principal principal-type timestamp key-version number key-type key-length encrypted-keytab*

no kerberos srvtab entry *kerberos-principal principal-type*

Syntax Description

| | |
|---------------------------|--|
| <i>kerberos-principal</i> | A service on the router. |
| <i>principal-type</i> | Version of the Kerberos SRVTAB. |
| <i>timestamp</i> | Number representing the date and time the SRVTAB entry was created. |
| <i>key-version number</i> | Version of the encryption key format. |
| <i>key-type</i> | Type of encryption used. |
| <i>key-length</i> | Length, in bytes, of the encryption key. |
| <i>encrypted-keytab</i> | Secret key the router shares with the KDC. It is encrypted with the private Data Encryption Standard (DES) key (if available) when you write out your configuration. |

Command Modes

Global configuration

Command History

| Release | Modification |
|---------|------------------------------|
| 11.2 | This command was introduced. |

Usage Guidelines

When you use the **kerberos srvtab remote** command to copy the SRVTAB file from a remote host (generally the KDC), it parses the information in this file and stores it in the router's running configuration in the **kerberos srvtab entry** format. The key for each SRVTAB entry is encrypted with a private DES key if one is defined on the router. To ensure that the SRVTAB is available (that is, that it does not need to be acquired from the KDC) when you reboot the router, use the **write memory** router configuration command to write the router's running configuration to NVRAM.

If you reload a configuration, with a SRVTAB encrypted with a private DES key, on a router that does not have a private DES key defined, the router displays a message informing you that the SRVTAB entry has been corrupted, and discards the entry.

If you change the private DES key and reload an old version of the router's configuration that contains SRVTAB entries encrypted with the old private DES keys, the router will restore your Kerberos SRVTAB entries, but the SRVTAB keys will be corrupted. In this case, you must delete your old Kerberos SRVTAB entries and reload your Kerberos SRVTABs on to the router using the **kerberos srvtab remote** command.

Although you can configure **kerberos srvtab entry** on the router manually, generally you would not do this because the keytab is encrypted automatically by the router when you copy the SRVTAB using the **kerberos srvtab remote** command.

Examples

In the following example, host/new-router.domain.com@DOMAIN.COM is the host, 0 is the type, 817680774 is the timestamp, 1 is the version of the key, 1 indicates the DES is the encryption type, 8 is the number of bytes, and .cCN.YoU.okK is the encrypted key:

```
kerberos srvtab entry host/new-router.domain.com@DOMAIN.COM 0 817680774 1 1 8
.cCN.YoU.okK
```

Related Commands

| Command | Description |
|-------------------------------|---|
| kerberos srvtab remote | Retrieves a krb5 SRVTAB file from the specified host. |
| key config-key | Defines a private DES key for the router. |

kerberos srvtab remote

To retrieve a krb5 SRVTAB file from the specified host, use the **kerberos srvtab remote** global configuration command.

```
kerberos srvtab remote {hostname | ip-address} filename
```

Syntax Description

| | |
|-------------------|--|
| <i>hostname</i> | Machine with the Kerberos SRVTAB file. |
| <i>ip-address</i> | IP address of the machine with the Kerberos SRVTAB file. |
| <i>filename</i> | Name of the SRVTAB file. |

Command Modes

Global configuration

Command History

| Release | Modification |
|---------|------------------------------|
| 11.2 | This command was introduced. |

Usage Guidelines

When you use the **kerberos srvtab remote** command to copy the SRVTAB file from the remote host (generally the KDC), it parses the information in this file and stores it in the router's running configuration in the **kerberos srvtab entry** format. The key for each SRVTAB entry is encrypted with the private Data Encryption Standard (DES) key if one is defined on the router. To ensure that the SRVTAB is available (that is, that it does not need to be acquired from the KDC) when you reboot the router, use the **write memory** configuration command to write the router's running configuration to NVRAM.

Examples

The command in the following example copies the SRVTAB file residing on b1.domain.com to a router named s1.domain.com:

```
kerberos srvtab remote b1.domain.com s1.domain.com-new-srvtab
```

Related Commands

| Command | Description |
|------------------------------|--|
| kerberos srvtab entry | Retrieves a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration. |
| key config-key | Defines a private DES key for the router. |

key config-key

To define a private DES key for the router, use the **key config-key** global configuration command. Use the **no** form of this command to delete a private DES key for the router.

key config-key 1 *string*

Syntax Description

string Private DES key (can be up to eight alphanumeric characters).

Defaults

No DES-key defined

Command Modes

Global configuration

Command History

| Release | Modification |
|---------|----------------------------|
| 11.2 | This command was released. |

Usage Guidelines

This command defines a private DES key for the router that will not show up in the router configuration. This private DES key can be used to DES-encrypt certain parts of the router's configuration.



Caution

The private DES key is unrecoverable. If you encrypt part of your configuration with the private DES key and lose or forget the key, you will not be able to recover the encrypted data.

Examples

The command in the following example sets *keyxx* as the private DES key on the router:

```
key config-key 1 keyxx
```

Related Commands

| Command | Description |
|-------------------------------|--|
| kerberos srvtab entry | Retrieves a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration. |
| kerberos srvtab remote | Retrieves a krb5 SRVTAB file from the specified host. |

show kerberos creds

To display the contents of your credentials cache, use the **show kerberos creds** privileged EXEC command.

show kerberos creds

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|---------|------------------------------|
| 11.1 | This command was introduced. |

Usage Guidelines

The **show kerberos creds** command is equivalent to the UNIX klist command.

When users authenticate themselves with Kerberos, they are issued an authentication ticket called a *credential*. The credential is stored in a credential cache.

Examples

The following example displays entries in the credentials cache:

```
Router> show kerberos creds

Default Principal: user@domain.com
Valid Starting      Expires              Service Principal
18-Dec-1995 16:21:07  19-Dec-1995 00:22:24  krbtgt/DOMAIN.COM@DOMAIN.COM
```

The following example returns output that acknowledges that credentials do *not* exist in the credentials cache:

```
Router> show kerberos creds

No Kerberos credentials
```

Related Commands

| Command | Description |
|-----------------------------|--|
| clear kerberos creds | Deletes the contents of the credentials cache. |