



# Lock-and-Key Commands

---

This chapter describes lock-and-key commands. Lock-and-key security is a traffic filtering security feature that uses dynamic access lists. Lock-and-key is available for IP traffic only.

Refer to the *Command Reference Master Index* or search online to find complete descriptions of other commands used when configuring lock-and-key.

For lock-and-key configuration information, refer to the “Configuring Lock-and-Key Security (Dynamic Access Lists)” chapter in the *Security Configuration Guide*.

## access-enable

To enable the router to create a temporary access list entry in a dynamic access list, use the **access-enable EXEC** command.

```
access-enable [host] [timeout minutes]
```

### Syntax Description

|                               |   |
|-------------------------------|---|
| <b>host</b>                   | (Optional) Tells the software to enable access only for the host from which the Telnet session originated. If not specified, the software allows all hosts on the defined network to gain access. The dynamic access list contains the network mask to use for enabling the new network.  |
| <b>timeout <i>minutes</i></b> | (Optional) Specifies an idle timeout for the temporary access list entry. If the access list entry is not accessed within this period, it is automatically deleted and requires the user to authenticate again. The default is for the entries to remain permanently. We recommend that this value equal the idle timeout set for the WAN connection. |

### Command Mode

EXEC

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

This command enables the lock-and-key access feature.

You should always define either an idle timeout (with the **timeout** keyword in this command) or an absolute timeout (with the **timeout** keyword in the **access-list** command). Otherwise, the temporary access list entry will remain, even after the user terminates the session.

Use the `autocommand` command with the `access-enable` command to cause the `access-enable` command to execute when a user Telnets into the router.

## Example

The following example causes the software to create a temporary access list entry and tells the software to enable access only for the host from which the Telnet session originated. If the access list entry is not accessed within 2 minutes, it is deleted.

```
autocommand access-enable host timeout 2
```

## Related Commands

`access-list (extended)`  
`autocommand`  
`show ip accounting`

## access-template

To manually place a temporary access list entry on a router to which you are connected, use the `access-template EXEC` command.

```
access-template [access-list-number | name] [dynamic-name] [source] [destination] [timeout minutes]
```

## Syntax Description

|                               |  |
|-------------------------------|--|
| <i>access-list-number</i>     | (Optional) Number of the dynamic access list.  |
| <i>name</i>                   | (Optional) Name of an IP access list. The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists.  |
| <i>dynamic-name</i>           | (Optional) Name of a dynamic access list.  |
| <i>source</i>                 | (Optional) Source address in a dynamic access list. The keywords <b>host</b> and <b>any</b> are allowed. All other attributes are inherited from the original access-list entry.   |
| <i>destination</i>            | (Optional) Destination address in a dynamic access list. The keywords <b>host</b> and <b>any</b> are allowed. All other attributes are inherited from the original access-list entry.  |
| <b>timeout</b> <i>minutes</i> | (Optional) Specifies a maximum time limit for each entry within this dynamic list. This is an absolute time, from creation, that an entry can reside in the list. The default is an infinite time limit and allows an entry to remain permanently. |

## Command Mode

EXEC

## Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

This command provides a way to enable the lock-and-key access feature.

You should always define either an idle timeout (with the **timeout** keyword in this command) or an absolute timeout (with the **timeout** keyword in the **access-list** command). Otherwise, the dynamic access list will remain, even after the user has terminated the session.

## Example

In the following example, the software enables IP access on incoming packets in which the source address is 172.29.1.129 and the destination address is 192.168.52.12. All other source and destination pairs are discarded.

```
access-template 101 payroll host 172.29.1.129 host 192.168.52.12 timeout 2
```

## Related Commands

- access-list (extended)
- autocommand
- clear access-template
- show ip accounting

## clear access-template

To manually clear a temporary access list entry from a dynamic access list, use the **clear access-template EXEC** command.

```
clear access-template [access-list-number | name] [dynamic-name] [source] [destination]
```

## Syntax Description

|                           |   |
|---------------------------|---|
| <i>access-list-number</i> | (Optional) Number of the dynamic access list from which the entry is to be deleted.   |
| <i>name</i>               | (Optional) Name of an IP access list from which the entry is to be deleted. The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists. |
| <i>dynamic-name</i>       | (Optional) Name of the dynamic access list from which the entry is to be deleted.   |
| <i>source</i>             | (Optional) Source address in a temporary access list entry to be deleted.   |
| <i>destination</i>        | (Optional) Destination address in a temporary access list entry to be deleted.  |

## Command Mode

EXEC

## Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

This command is related to the lock-and-key access feature. It clears any temporary access list entries that match the parameters you define.

## Example

The following example clears any temporary access list entries with a source of 172.20.1.12 from the dynamic access list named vendor:

```
clear access-template vendor 172.20.1.12
```

## Related Commands

access-list (extended)  
access-template  
show ip accounting