



## Multiple-Tier CA Hierarchies

---

Hierarchical public key infrastructure (PKI) has been enhanced to support multiple-tier certification authorities (CAs). Before multiple CAs were supported, the customer would have to establish the hierarchy by first configuring a root CA (which has a self-signed certificate that contains its own public key). Thereafter, subordinate CAs were enrolled with the root CA. This design limited the customer's CA hierarchy to two tiers because each CA had to be a direct subordinate of the root CA.

Multiple-tier CA support eliminates the following restrictions:

- Two-tier limitation. Cisco IOS now supports any number of CA tiers.
- Mandatory root CA configuration. Configuring the root CA is now optional.
- Customers are no longer required to start configuring CAs from the top tier (root CA). That is, IP Security (IPSec) connections can now be established between any two routers from any tier if the routers are configured to share at least one common CA (trustpoint) within the hierarchy.

### Feature History for Multiple-Tiered CA Hierarchies

| Release   | Modification                     |
|-----------|----------------------------------|
| 12.2(15)T | This enhancement was introduced. |

## Contents

- [How to Configure Multiple-Tier CAs, page 1](#)
- [Configuration Examples for Multiple-Tiered CAs, page 3](#)
- [Additional References, page 4](#)

## How to Configure Multiple-Tier CAs

This section shows how to configure trustpoints (or CAs) for a multiple-tier CA hierarchy.

- [Configuring CAs for Multiple-Tier Hierarchy, page 2](#)



---

**Corporate Headquarters:**  
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

## Configuring CAs for Multiple-Tier Hierarchy

In Cisco IOS software, each CA corresponds to a trustpoint. Thus, you should perform the following steps for each CA you want to configure within the hierarchy.

### Manually Accepting the Initial CA (Root or Subordinate) Certificate

When you configure the first root or subordinate CA within the CA hierarchy, you will be asked to manually accept the CA certificate because Cisco IOS PKI cannot cryptographically check the validity of the root or subordinate CA certificate.

After the root or subordinate CA certificate has been manually accepted, it will be stored in the trusted certificate and can now be used to validate additional certificates.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ca trustpoint *name***
4. **enrollment url *url***
5. **exit**
6. **crypto ca authenticate *name***

#### DETAILED STEPS

|        | Command or Action   | Purpose   |
|--------|---|---|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable  | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal  | Enters global configuration mode.   |
| Step 3 | <b>crypto ca trustpoint <i>name</i></b><br><br><b>Example:</b><br>Router(config)# crypto ca trustpoint CA11                 | Declares a CA and enters ca-trustpoint configuration mode.  |
| Step 4 | <b>enrollment url <i>url</i></b><br><br><b>Example:</b><br>Router(ca-trustpoint)# enrollment url<br>http://ciscoca-ultra:80 | Specifies the enrollment parameters of a CA.  |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(ca-trustpoint)# exit   | Exits ca-trustpoint configuration mode.   |

|        | Command or Action   | Purpose   |
|--------|---|---|
| Step 6 | <code>crypto ca authenticate name</code><br><br><b>Example:</b><br>Router(config)# <code>crypto ca authenticate ms</code> | Authenticates the CA to your router by obtaining the self-signed certificate of the CA. |
| Step 7 | —   | Repeat these steps for each CA you want to configure within the hierarchy.              |

## Troubleshooting Tips

To verify information about your certificate and the certificate of the CA, use the `show crypto ca certificates EXEC` command.

# Configuration Examples for Multiple-Tiered CAs

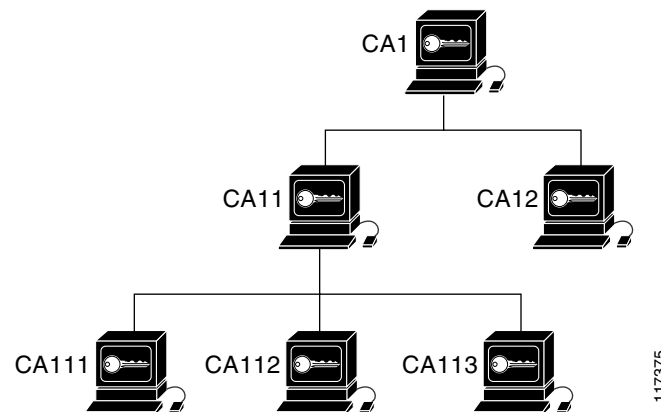
This section contains the following configuration example:

- [Configuring Multiple-Tiered CAs: Example, page 3](#)

## Configuring Multiple-Tiered CAs: Example

Figure 1 shows the enrollment relationships among CAs within a three-tiered hierarchy.

**Figure 1** Three-Tiered CA Hierarchy Sample Topology



Each CA corresponds to a trustpoint. For example, CA11 and CA12 are subordinate CAs, holding CA certificates that have been issued by CA1; CA111, CA112, and CA113 are also subordinate CAs, but their CA certificates have been issued by CA11.

On the basis of Figure 1, if a customer wants to configure CA11 and CA112 on a router, the customer should follow this example:

```

Router(config)# crypto ca trustpoint CA11
Router(ca-trustpoint)# enrollment url http://ciscoca-ultra:80
Router(ca-trustpoint)# exit
  
```

```

Router(config)# crypto ca authenticate ms
Certificate has the following attributes:
Fingerprint:84E470A2 38176CB1 AA0476B9 C0B4F478
% Do you accept this certificate? [yes/no]:y
Trustpoint CA certificate accepted.

Router(config)# crypto ca trustpoint CA112
Router(ca-trustpoint)# enrollment url http://kahului:80
Router(ca-trustpoint)# exit
Router (config)# crypto ca authenticate CA112
Certificate has the following attributes:
Fingerprint:9F6BDD67 14F643C6 D23BB000 63257CDE
Certificate validated - Signed by existing trustpoint CA certificate.
Trustpoint CA certificate accepted.

```

**Note**


---

CA112 has been automatically accepted because its validity can be checked via CA11.

---

## Additional References

The following sections provide references related to multiple-tiered CA hierarchies.

## Related Documents

| Related Topic            | Document Title  |
|--------------------------|---|
| Trustpoint configuration | <i>Trustpoint CLI</i> , Cisco IOS Release 12.2(8)T feature module   |
| CA information           | The chapter “Configuring Certification Authority Interoperability” in the <i>Cisco IOS Security Configuration Guide</i> |

## Standards

| Standards | Title |
|-----------|-------|
| None      | —     |

## MIBs

| MIBs | MIBs Link  |
|------|--|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs | Title |
|------|-------|
| None | —     |

## Technical Assistance

| Description  | Link  |
|--|---|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

