

Certificate Expiration and Auto-Enroll for Automatic Re-Enroll to Cisco IOS CA

Document ID: 50551

Introduction

Prerequisites

Requirements

Components Used

Conventions

When is a Digital Certificate Considered Expired or Not Expired?

Related Information

Introduction

All Digital Certificates have a built in expiration time in the certificate that is assigned by the issuing Certificate Authority (CA) server during enrollment. When a Digital Certificate is used for VPN IPSec authentication of ISAKMP, there is an automatic check of the communicating device's certificate expiration time and the system time on the device (VPN endpoint). This ensures that a certificate used is valid and has not expired. It is also why you *must* set the internal clock on each VPN endpoint (router). If Network Time Protocol (NTP) (or Simple Network Time Protocol [SNTP]) is not possible on the VPN crypto routers, then use the manual `set clock` command.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on all routers that run the cXXXX-advsecurityk9-mz.123-5.9.T image for that respective platform .

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

When is a Digital Certificate Considered Expired or Not Expired?

- A certificate is expired (invalid) if the system time is after the certificate expiration time or before the issued time of the certificate.
- A certificate is not expired (valid) if the system time is at or between the certificate's issued time and the certificate's expired time.

The purpose of the Auto-enroll feature is to provide the CA administrator with a mechanism to allow a currently enrolled router to automatically re-enroll with its CA server on a configured percent of the lifetime of the router certificate. This is an important feature for the manageability / supportability of the certificates as a control mechanism. If you used a particular CA to issue certificates to potentially thousands of branch VPN routers with a one year lifetime (without Auto-enroll), then in exactly one year of the issued time, all of the certificates expire and all of the branches lose connectivity through IPSec. Alternatively, if the Auto-enroll feature is set to "auto-enroll 70", as in this example, then in 70% of the lifetime of the issued certificate (1 year), each router automatically issues a new enrollment request to the Cisco IOS® CA server listed in the trustpoint.

Note: One exception to the Auto-enroll feature is that if it is set to *less than or equal to 10*, then it is in minutes. If it is *greater than 10*, then it is a percentage of the certificate's lifetime.

There are some caveats the Cisco IOS CA administrator needs to be aware of with Auto-enroll. The administrator needs to execute these actions for the re-enrollment to be successful:

1. Manually grant or reject each re-enrollment request on the Cisco IOS CA server (unless "grant auto" is used on the Cisco IOS CA server).
 - ◆ The Cisco IOS CA server still needs to either grant or reject each of these requests (with the assumption that the Cisco IOS CA does not have "grant auto" enabled). However, no administrative action on the enrolling router is required to start the re-enrollment process.
2. Save the new re-enrolled certificate in the re-enrolling VPN router, if appropriate.
 - ◆ If there are no unsaved configuration changes pending in the router, then the new certificate is automatically saved to the Non-Volatile RAM (NVRAM). The new certificate is written in the NVRAM and the previous certificate is removed.
 - ◆ If there are unsaved configuration changes pending, then you must issue the **copy run start** command on the enrolling router in order to save the configuration changes and the new re-enrolled certificate into the NVRAM. Once the **copy run start** command is completed, then the new certificate is written in the NVRAM and the previous certificate is removed.

Note: When a new re-enrollment is successful, that does *not* revoke the previous certificate for that enrolled device on the CA server. When VPN devices communicate, they send each other the Certificate Serial number (a unique number).

Note: For example, if you are at 70% of the certificate's lifetime and a VPN branch was to re-enroll with the CA, that CA has two certificates for that hostname. However, the enrolling router only has one (the newer one). If you choose to, you can administratively revoke the old certificate, or allow it to expire normally.

Note: The newer code versions of the Auto-enroll feature have an option to "regenerate" the key-pairs used for enrollment.

- ◇ This option is "not default" to regenerate key-pairs.
- ◇ If this option was chosen, be aware of Cisco bug ID CSCea90136. This bug fix allows for the new key-pair to be put in temporary files while the new certificate enrollment takes place over an existing IPSec tunnel (that is using the old key-pair).

Auto-enroll has the option to generate new keys at certification renewal time. Currently this causes a loss of service during the time it takes to obtain a new certificate. This is because there is a new key but no certificate that matches it.

This feature retains the old key and certificate until the new certificate is available.

Automatic key generation is also implemented for manual enrollment. Keys are generated (as needed) for automatic or manual enrollment.

- Version found – 12.3PIH03
- Version to be fixed in – 12.3T
- Version applied to – 12.3PI03
- Integrated in – None

For additional information, contact Cisco Technical Support.

Related Information

- [IPSec Support Page](#)
 - [Technical Support – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jan 14, 2008

Document ID: 50551
