

ACS Solution Engine (Appliance) for HTTPS Management Configuration Example

Document ID: 49941

Contents

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Configure

Verify

Troubleshoot

- Known Issue

Related Information

Introduction

This document describes how to set up the Cisco Secure ACS Solution Engine (SE) for HTTPS management.

Prerequisites

Requirements

Ensure that you meet this requirement before you attempt this configuration:

- Web administration access to both the Cisco Secure ACS SE and the Microsoft CA server

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure ACS SE 3.2.2. build 5
- Microsoft 2000 Stand Alone CA server
- Microsoft 2000 Enterprise CA Server

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

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Configure

This document uses these configurations steps:

1. Login and click **System Configuration**.

Address <http://172.18.124.102:1547/index2.htm>

CISCO SYSTEMS

Cisco Secure ACS v3.2

Select "Log Off" to end the administration session.

CiscoSecure ACS v3.2 offers support for multiple AAA Clients and advanced TACACS+ and RADIUS features. It also supports several methods of authorization, authentication, and accounting (AAA) including several one-time-password cards. For more information on CiscoSecure products and upgrades, please visit <http://www.cisco.com>.

CiscoSecure ACS
Release 3.2(2) Build 5
Copyright ©2003 Cisco Systems, Inc.
Copyright ©1998 RSA Data Security Australia Pty Ltd. All rights reserved
Copyright ©1991-1992 RSA Data Security, Inc. MD5 Message-Digest Algorithm. All rights reserved.
Copyright ©1989, 1993 The Regents of the University of California. All rights reserved
Copyright ©1986 University of Toronto. All rights reserved.
Copyright ©1985-2000 Microsoft Visual C++ Version 6.0. All rights reserved.
Copyright ©1997-2000 InstallShield Software Corporation. All rights reserved.
All other trademarks, service marks, registered trademarks, or registered service marks mentioned in this document are the property of their respective owners. Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

2. Click **ACS Certificate Setup**.

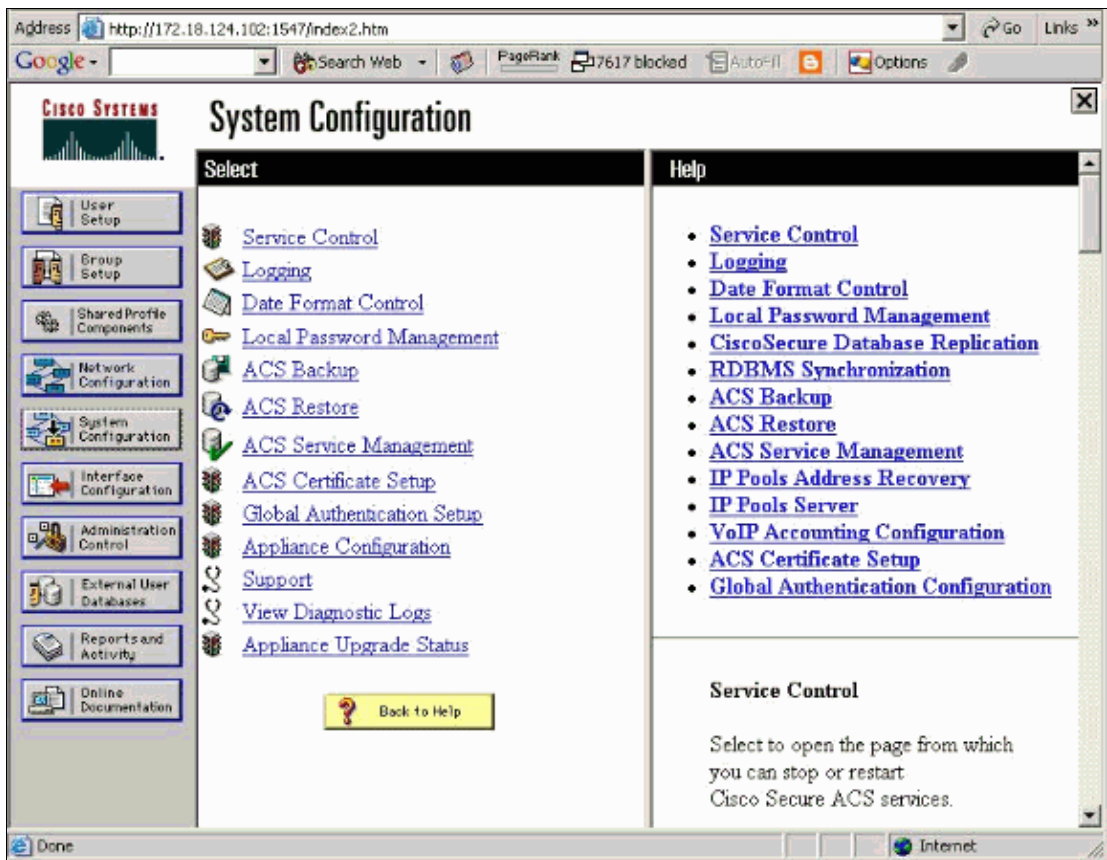
Address <http://172.18.124.102:1547/index2.htm>

System Configuration

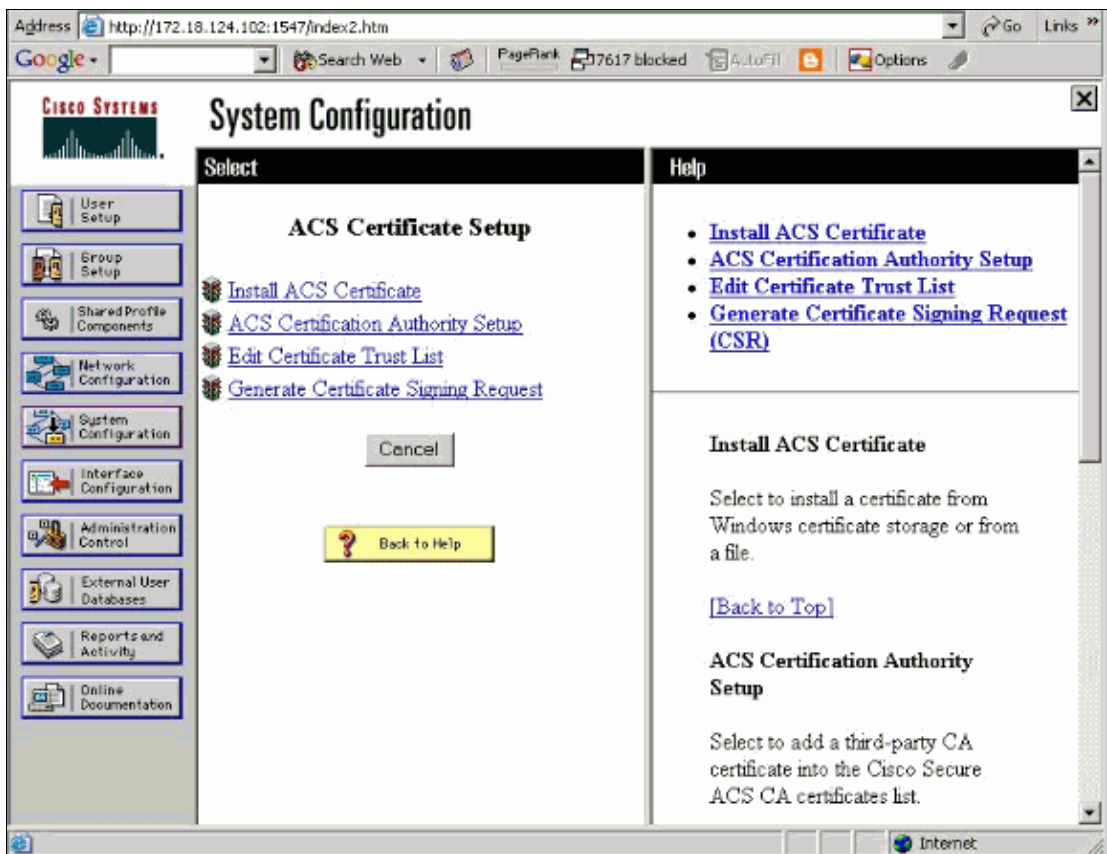
Select	Help
<ul style="list-style-type: none">Service ControlLoggingDate Format ControlLocal Password ManagementACS BackupACS RestoreACS Service ManagementACS Certificate SetupGlobal Authentication SetupAppliance ConfigurationSupportView Diagnostic LogsAppliance Upgrade Status	<ul style="list-style-type: none">Service ControlLoggingDate Format ControlLocal Password ManagementCiscoSecure Database ReplicationRDBMS SynchronizationACS BackupACS RestoreACS Service ManagementIP Pools Address RecoveryIP Pools ServerVoIP Accounting ConfigurationACS Certificate SetupGlobal Authentication Configuration

Service Control

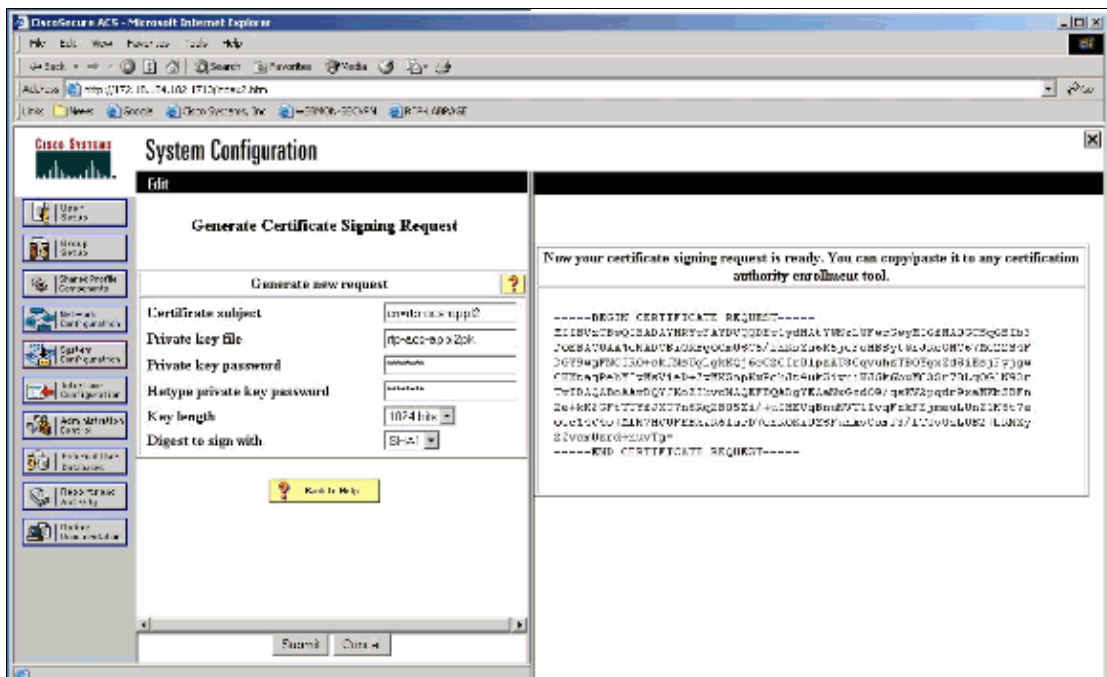
Select to open the page from which you can stop or restart Cisco Secure ACS services.



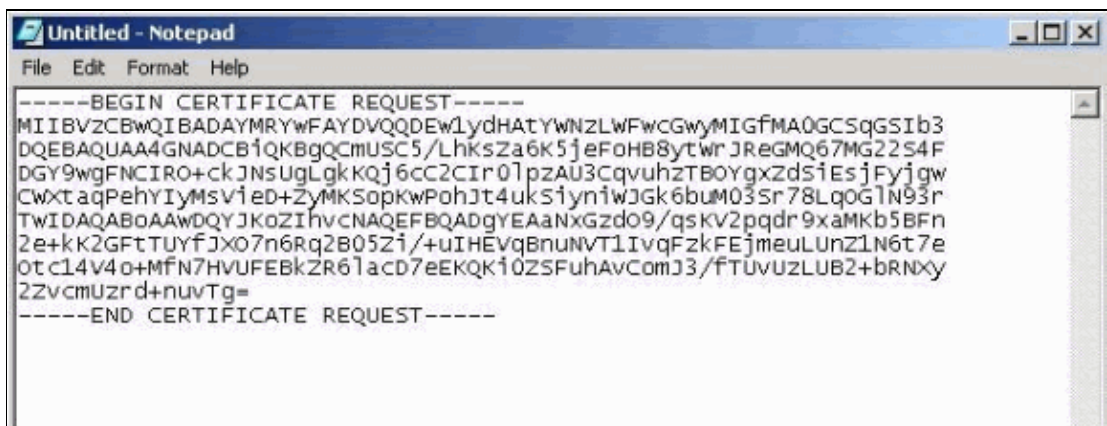
3. Click **Generate Certificate Signing Request**.



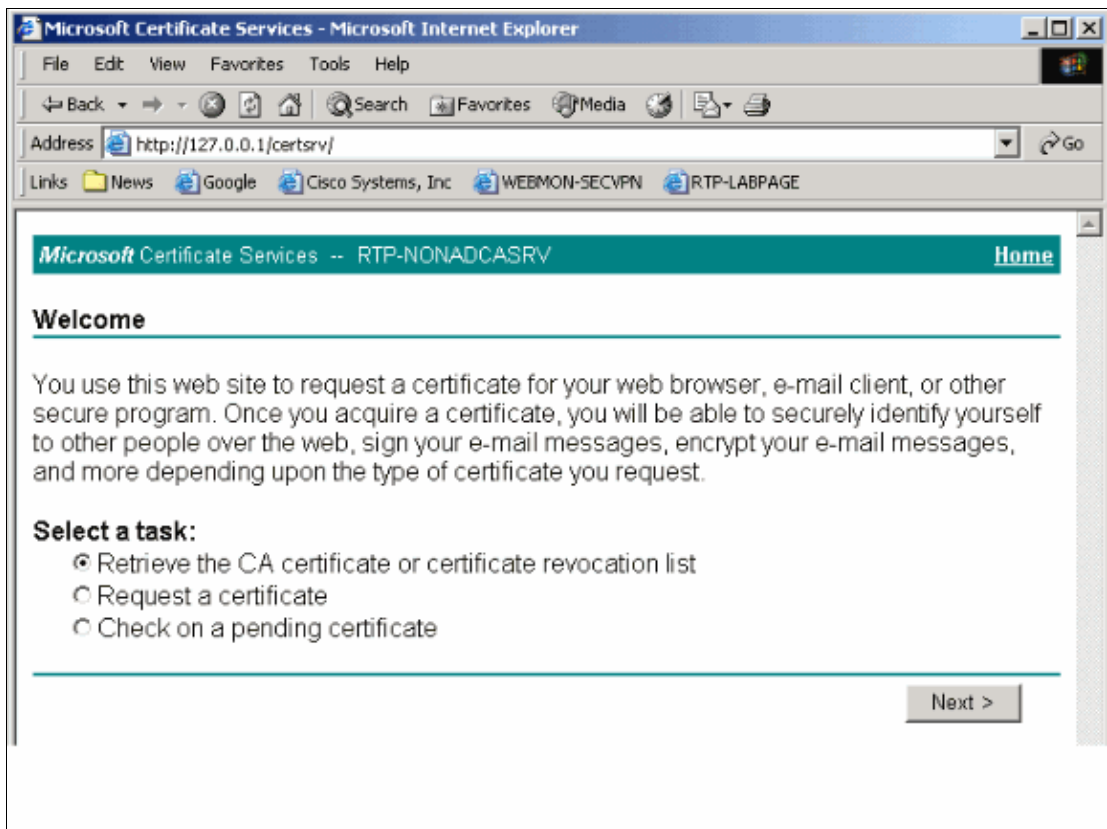
4. Fill out the form as you see here, click **Submit**, and note that your Certificate Signing Request is now ready by viewing it on the right-hand side of the window.



5. Copy the Certificate Signing Request to a Notepad file for use during a later step.

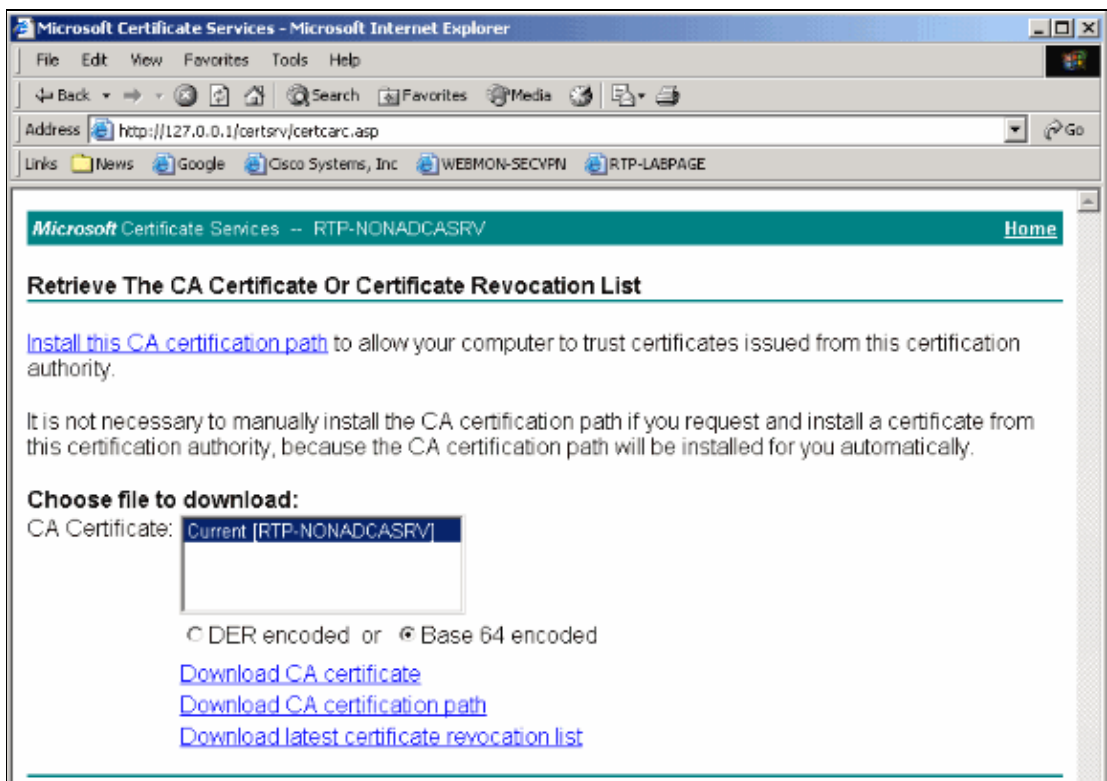


6. Browse to your Microsoft CA Server web page.
7. Select **Retrieve the CA certificate or certificate revocation list** to download the CA Server Certificate.

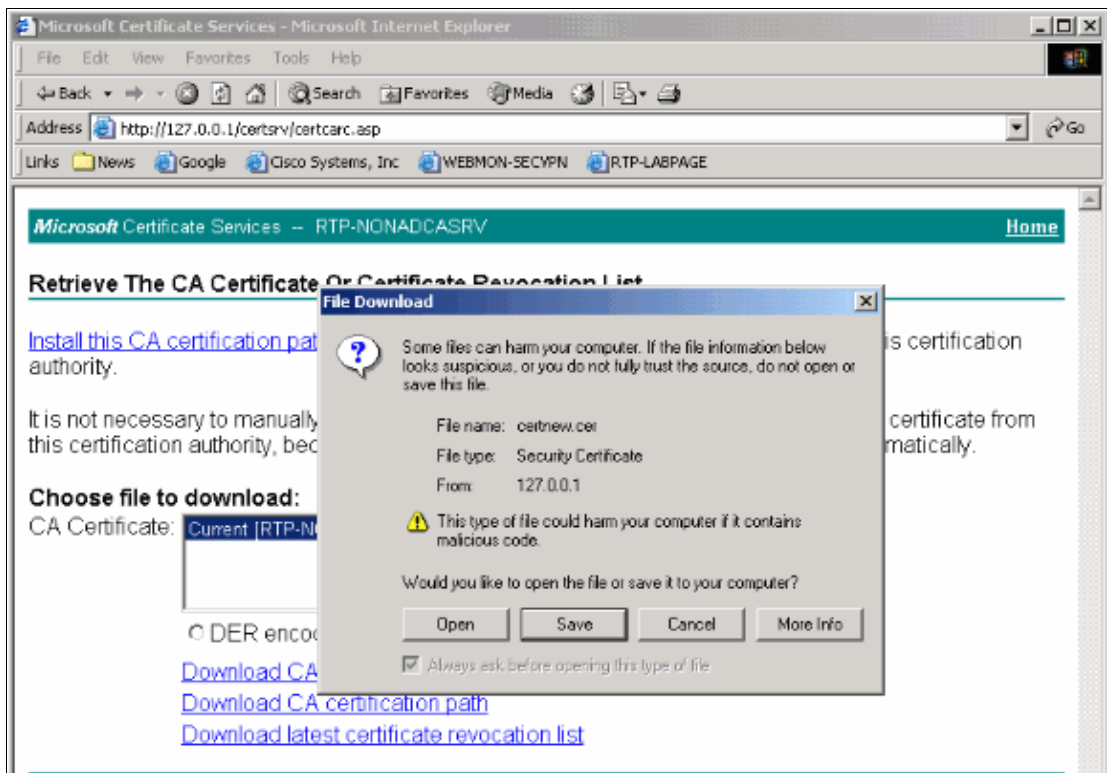


8. Click **Next**.

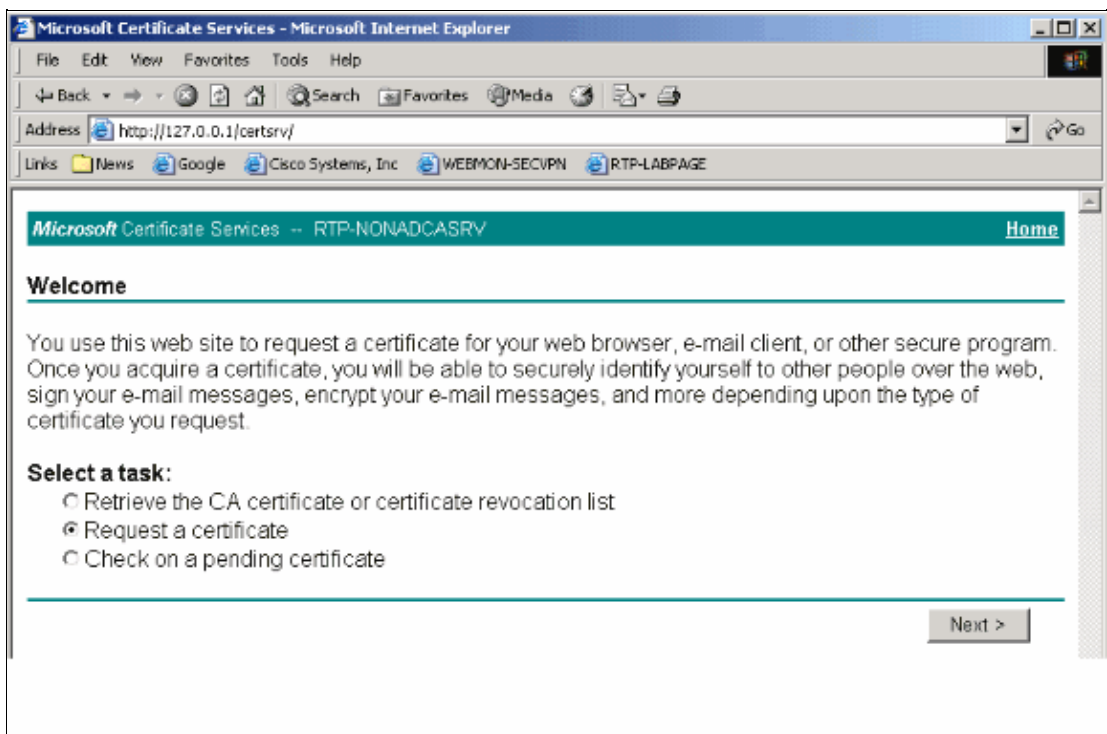
9. Select **Base 64 Encoded**.



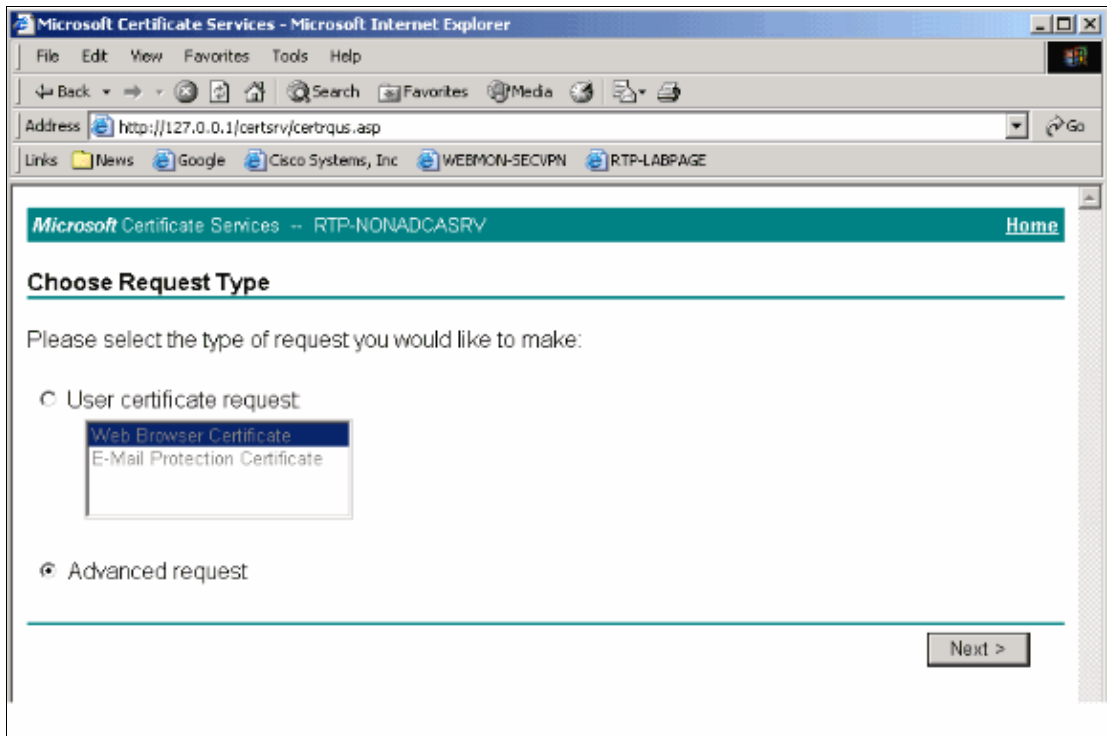
10. Click **Download CA certificate**.



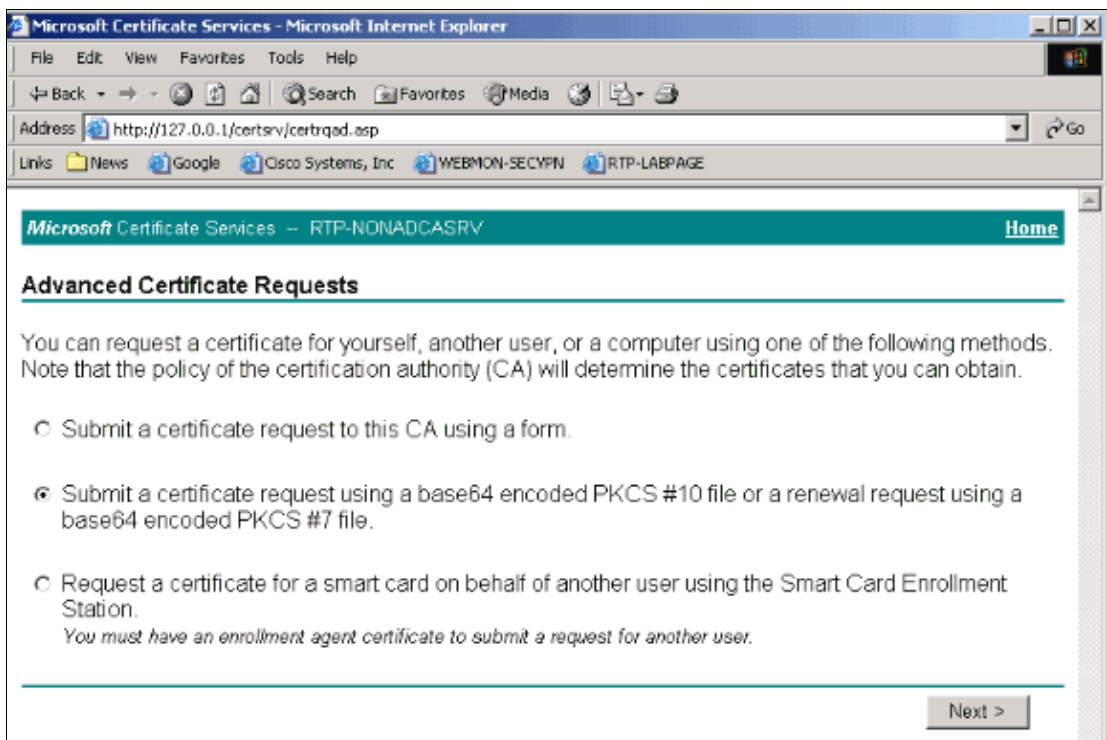
11. Click **Save** and rename the CA Server Certificate from certnew.cer to a name that is easy to remember. This example uses **ca-cert.cer**. After the file is renamed, save this ca-cert.cer to the FTP server's root directory.
12. Browse back to the CA Server's web page.



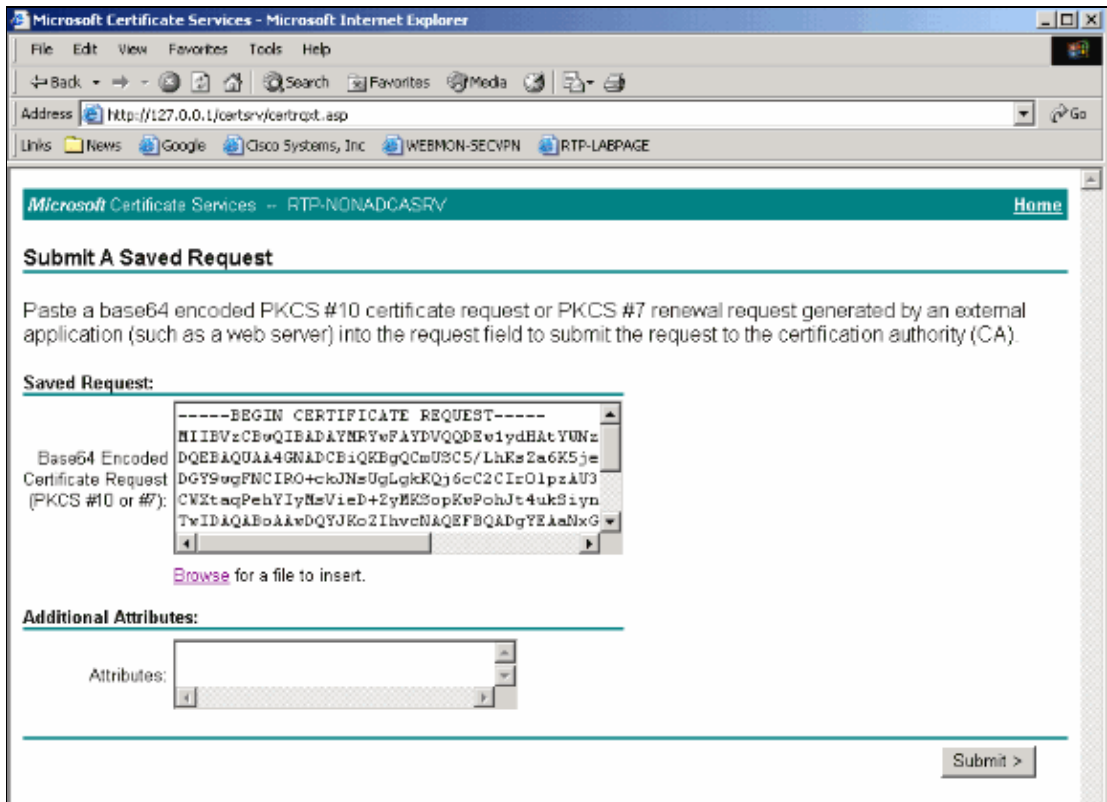
13. Click **Next** and select **Advanced Request**.



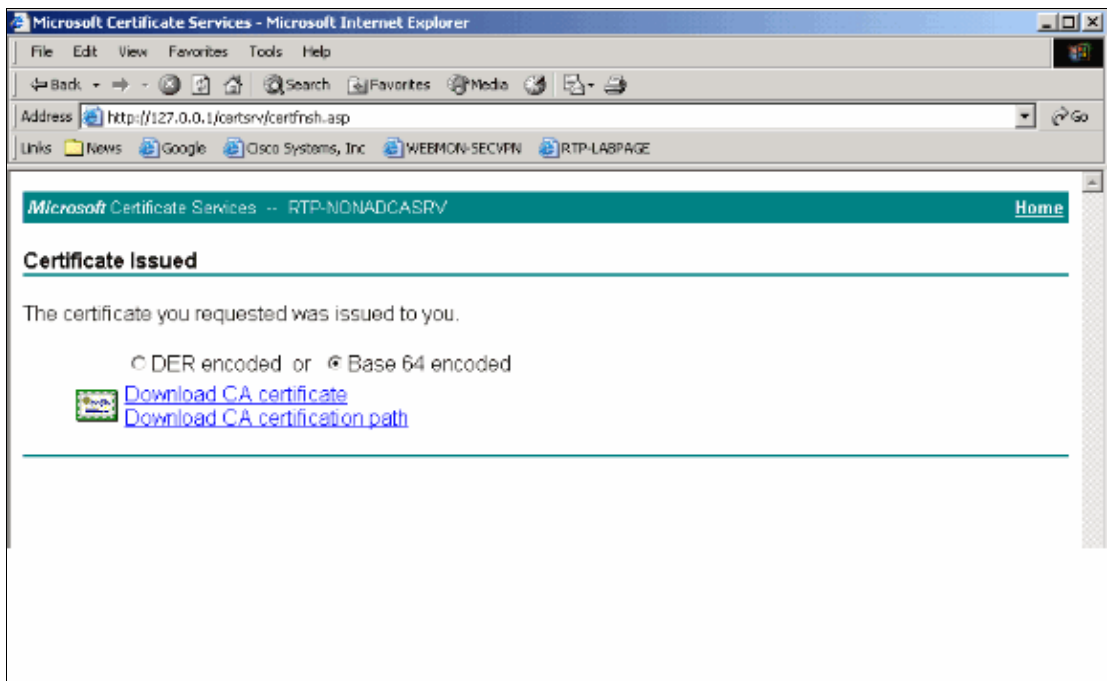
14. Click **Next** and select **Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.**



15. Click **Next** and paste in the Certificate Service Request that you copied to a Notepad file from step 6.



16. Click **Submit**.
17. Select **Base 64 encoded** and click **Download CA certificate**.



18. Click **Save** and rename this certificate from certnew.cer to a name that you can remember. This example uses **acs-cert.cer**. Save this file to your FTP server's root directory.
19. In your ACS Server browse to **System Configuration > ACS Certificate Setup > ACS Certification Authority Setup**, click **Download CA certificate file**, and fill out the Download File section completely.

CiscoSecure ACS - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print

Address http://172.18.124.102:1713/index2.htm

Links News Google Cisco Systems, Inc WEBMON-SECVPN RTP-LABPAGE

CISCO SYSTEMS

System Configuration

Edit

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration**
- Interface Configuration
- Administration Control
- External User Databases
- Reports and Activity
- Online Documentation

Download CA Certificate File

Download File ?

FTP Server 172.18.173.67

Login ftpuser

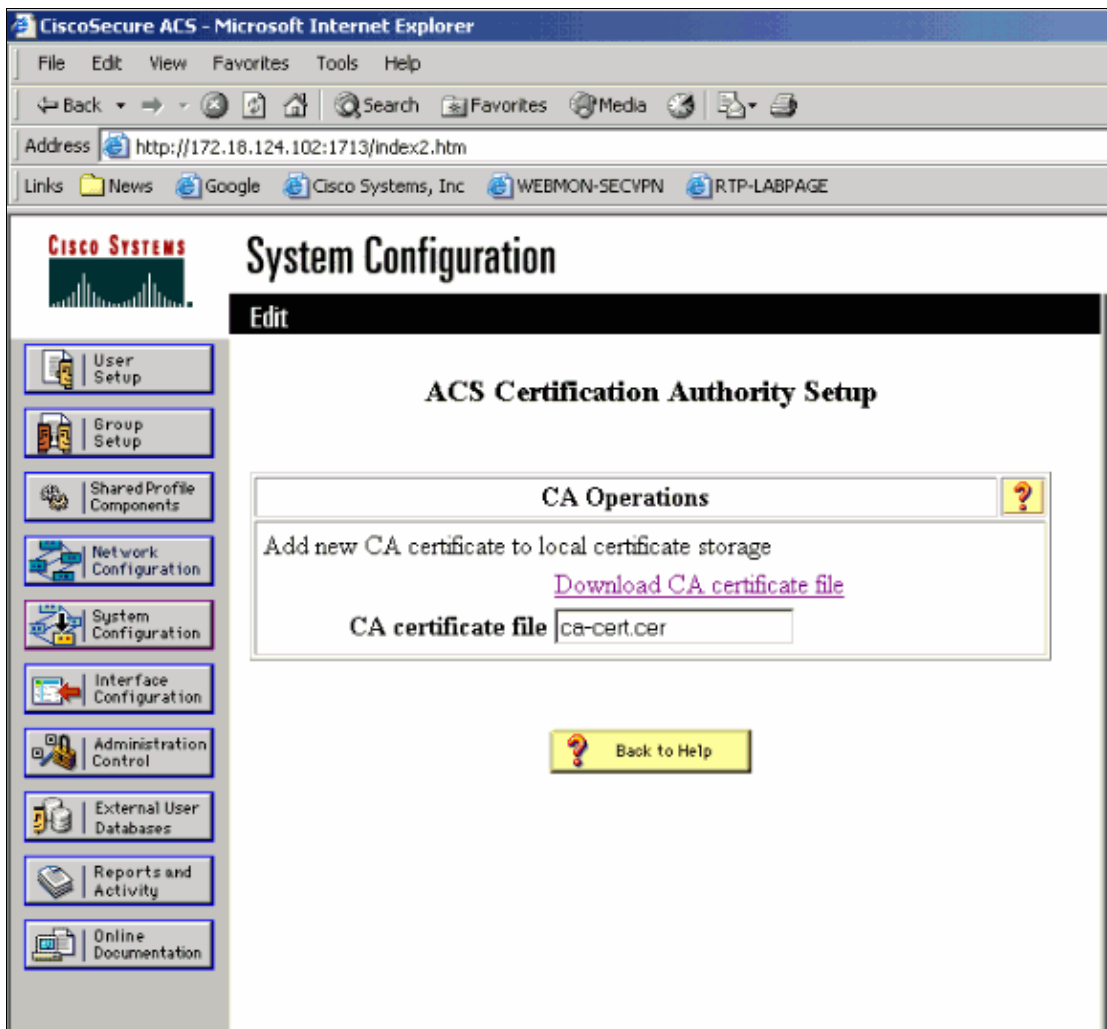
Password [REDACTED]

Directory /

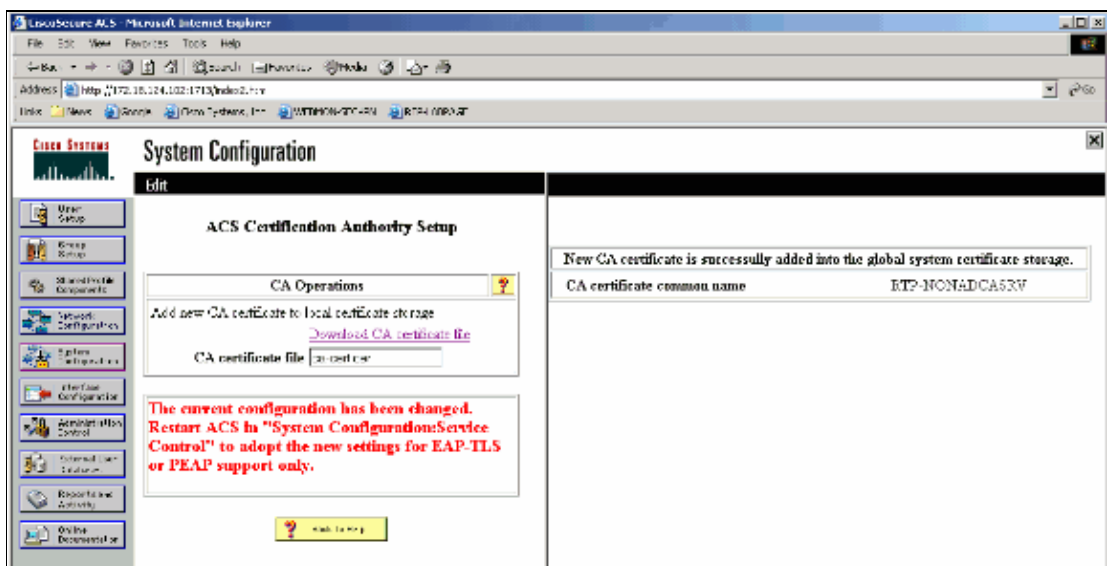
File ca-cert.cer

? Back to Help

20. Click **Submit**.



21. Click **Submit** again.



22. Select **System Configuration > ACS Certificate Setup > Install ACS Certificate** and click **Download certificate file**.

23. Fill out the Download File section completely.

CiscoSecure ACS - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print

Address http://172.18.124.102:1713/index2.htm

Links News Google Cisco Systems, Inc WEBMON-SECVPN RTP-LABPAGE

CISCO SYSTEMS

System Configuration

Edit

Download Certificate File

Download File ?

FTP Server 172.18.173.67

Login ftpuser

Password [REDACTED]

Directory /

File acs-cert.cer

? Back to Help

User Setup

Group Setup

Shared Profile Components

Network Configuration

System Configuration

Interface Configuration

Administration Control

External User Databases

Reports and Activity

Online Documentation

24. Click **Submit**.

CiscoSecure ACS - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print

Address http://172.18.124.102:1713/index2.htm

Links News Google Cisco Systems, Inc WEBMON-SECVPN RTP-LABPAGE

CISCO SYSTEMS

System Configuration

Edit

User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Reports and Activity
Online Documentation

Install ACS Certificate

The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only.

Install new certificate

Read certificate from file

[Download certificate file](#)

Certificate file

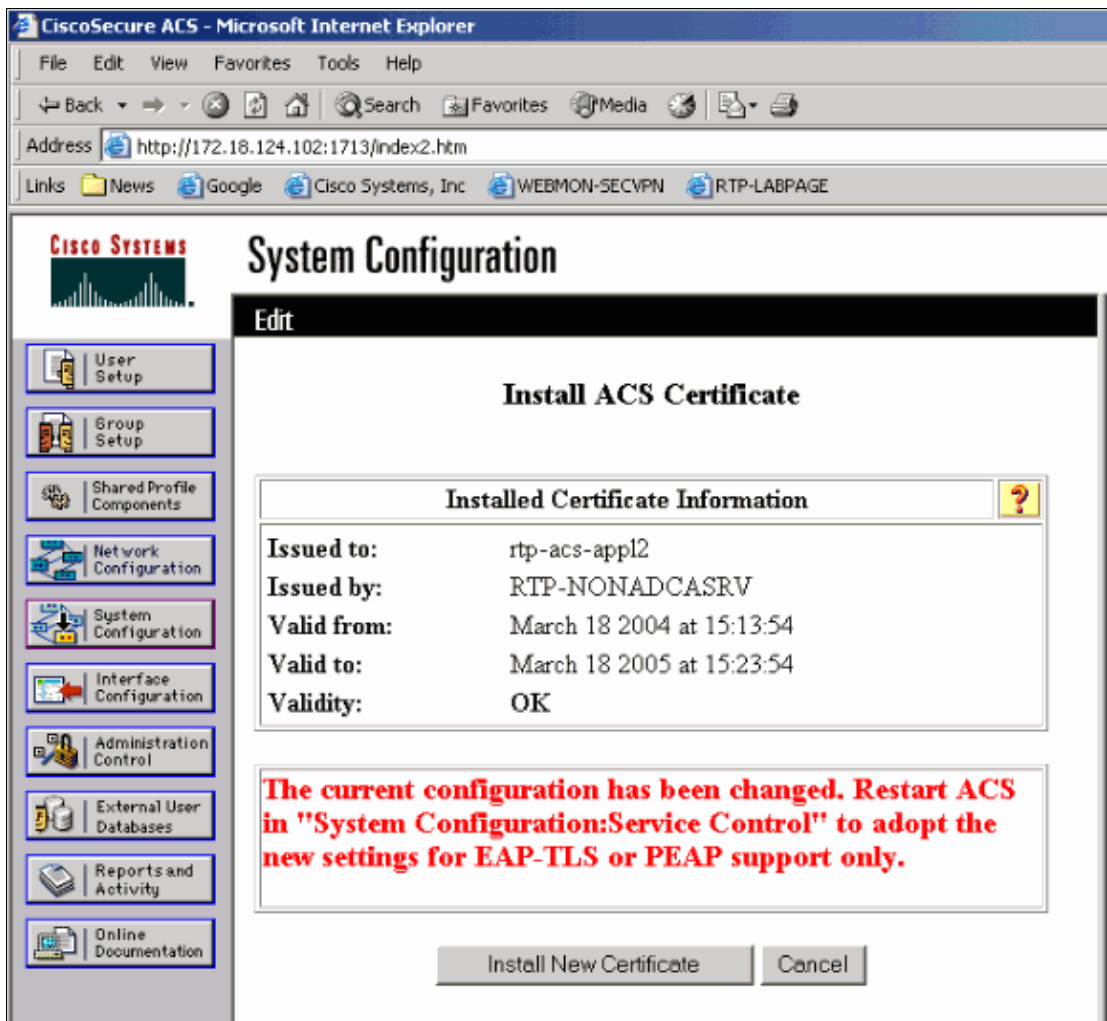
[Download private key file](#)

Private key file

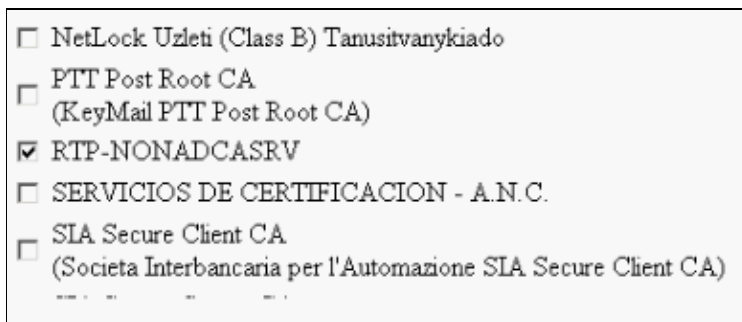
Private key password

[Back to Help](#)

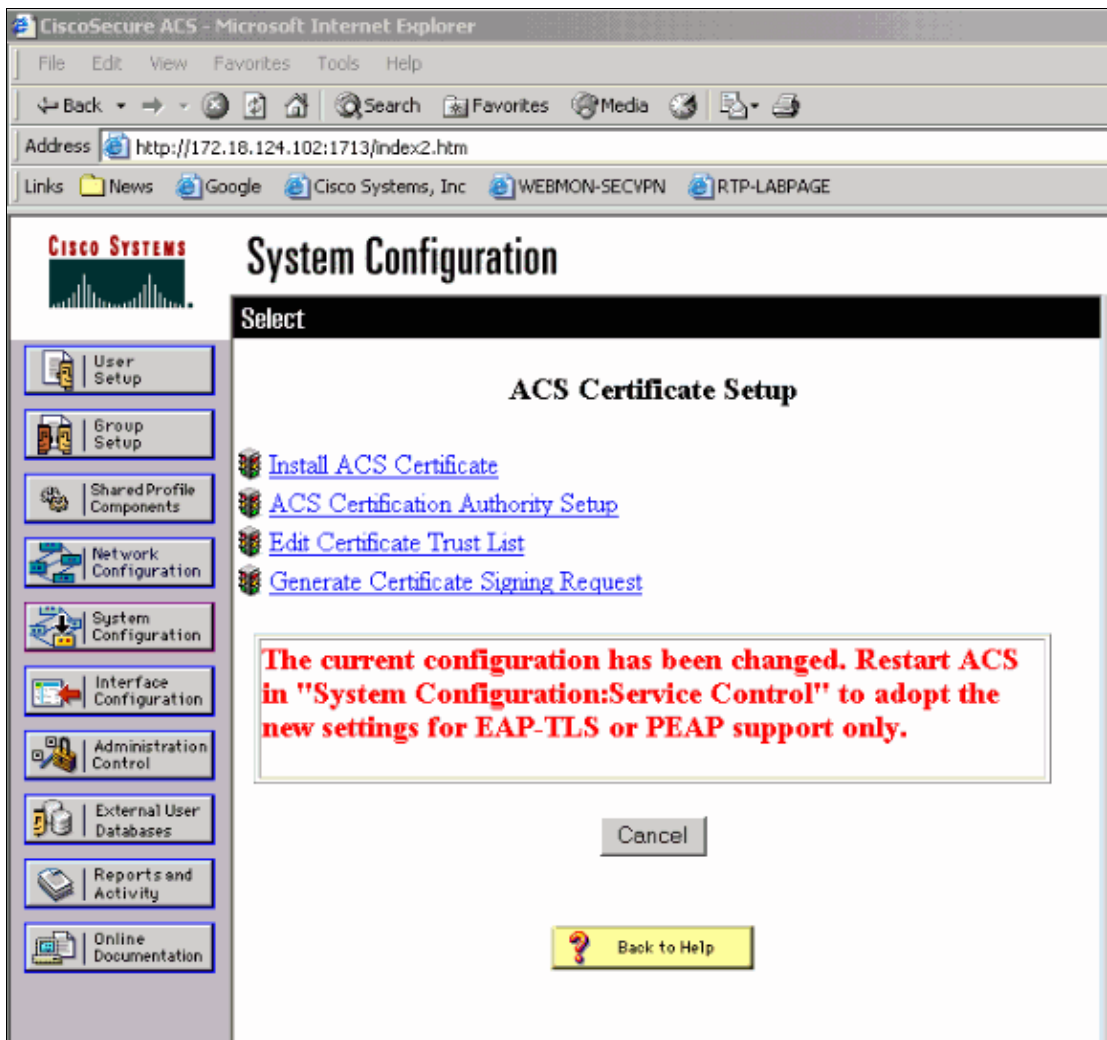
25. Click **Submit**.



26. Select **System Configuration > ACS Certificate Setup > Edit Certificate Trust List** and verify your CA server is listed. Once it is found, check the box next to the name.



27. Click **Submit**.



28. Select **System Configuration** > **Service Control** and click **Restart**.
29. Select **Administration Control** > **Access Policy** and under the HTTP Configuration section under Secure Socket Layer Setup, check **Use HTTPS Transport for Administration Access**. Once this is complete click **Submit**. Your ACS SE is now able to be used via an SSL browser session.

CISCO SYSTEMS

Administration Control

	Start IP Address	End IP Address
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

HTTP Configuration

HTTP Port Allocation

Allow any TCP ports to be used for Administration HTTP Access
 Restrict Administration Sessions to the following port range From Port to Port

Secure Socket Layer Setup

Use HTTPS Transport for Administration Access

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Known Issue

If you see the Can't initialize HTTPS transport: server or certification authority certificate is not installed error, your ID certificate is not installed.

Related Information

- [Documentation for Cisco Secure ACS Appliance](#)
 - [Cisco Secure ACS SE Support Page](#)
 - [Administering the Cisco Secure ACS Appliance](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

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

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jun 14, 2006

Document ID: 49941
