

ACS Kimlik Sunucusu ile PEAP Kurulumu ve Active Directory Entegrasyonu

Ahmet UNCU
İTÜ/BİDB

Gökhan AKIN
İTÜ/BİDB - ULAK/CSIRT

İSTANBUL - 2008

ACS'ye HTTP üzerinden bağlanmak

CiscoSecure ACS - Mozilla Firefox

Dosya Düzen Görünüm Geçmiş Yer İmleri Araçlar Yardım

http://127.0.0.1:3585/

İlk Adım Haberler

CISCO SYSTEMS

Cisco Secure ACS v4.0

Select "Log Off" to end the administration session.

CiscoSecure ACS v4.0 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 4.0(1) Build 27
Copyright ©2005 Cisco Systems, Inc.
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.

Applet appPing started

Sunucuda Sertifikanın Oluşturulması (1)

The screenshot displays the CiscoSecure ACS System Configuration web interface in a Mozilla Firefox browser. The browser's address bar shows the URL <http://127.0.0.1:3585/>. The page title is "System Configuration" and the main heading is "ACS Certificate Setup".

The left sidebar contains a navigation menu with the following items:

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

The main content area is titled "ACS Certificate Setup" and lists the following options:

- Install ACS Certificate
- ACS Certification Authority Setup
- Edit Certificate Trust List
- Certificate Revocation Lists
- Generate Certificate Signing Request
- Generate Self-Signed Certificate

Below the list are "Cancel" and "Back to Help" buttons. The right sidebar provides detailed instructions for each option:

- Install ACS Certificate**: Select to install a certificate from Windows certificate storage or from a file. [Back to Top]
- ACS Certification Authority Setup**: Select to add a third-party CA certificate into the ACS CA certificates list. [Back to Top]
- Edit Certificate Trust List**: You can specify which third-party certificate authorities (CAs) ACS should trust when authenticating users with certificate-based protocol. If a user's certificate is from a CA that you have not specifically configured ACS to trust, authentication fails. [Back to Top]
- Certificate Revocation Lists**: You can configure ACS to retrieve certificate revocation lists (CRLs) from CAs that are enabled on the Certificate Trust List. [Back to Top]
- Generate Certificate Signing Request**: You can use ACS to generate a certificate signing request (CSR). Once you have generated a CSR, you can submit it to a certificate authority to receive your certificate.

The bottom status bar shows "Tamam".

Sunucuda Sertifikanın Oluşturulması (2)

The screenshot shows the CiscoSecure ACS System Configuration interface in Mozilla Firefox. The page is titled "Generate Certificate Signing Request" and is in "Edit" mode. The main form contains the following fields:

- Certificate subject: CN=peapacs.cc.itu.ed
- Private key file: c:\key.ini
- Private key password: *****
- Retype private key password: *****
- Key length: 2048 bits
- Digest to sign with: SHA1

Below the form is a "Back to Help" button. At the bottom of the form are "Submit" and "Cancel" buttons. The left sidebar contains navigation options: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The right sidebar contains a list of links: Certificate subject, Private key file, Private key password, Retype private key password, Key length, and Digest to sign with. Below the links is a paragraph explaining the CSR generation process and a table of valid fields for the "Certificate subject" box.

Field	Field Name	Min. Length	Max. Length	Required?
CN	commonName	1	64	Yes
OU	organizationalUnitName	—	—	No
O	organizationName	—	—	No
S	stateOrProvinceName	—	—	No
C	countryName	2	2	No
E	emailAddress	0	40	No
L	localityName	—	—	No

[Back to Top]

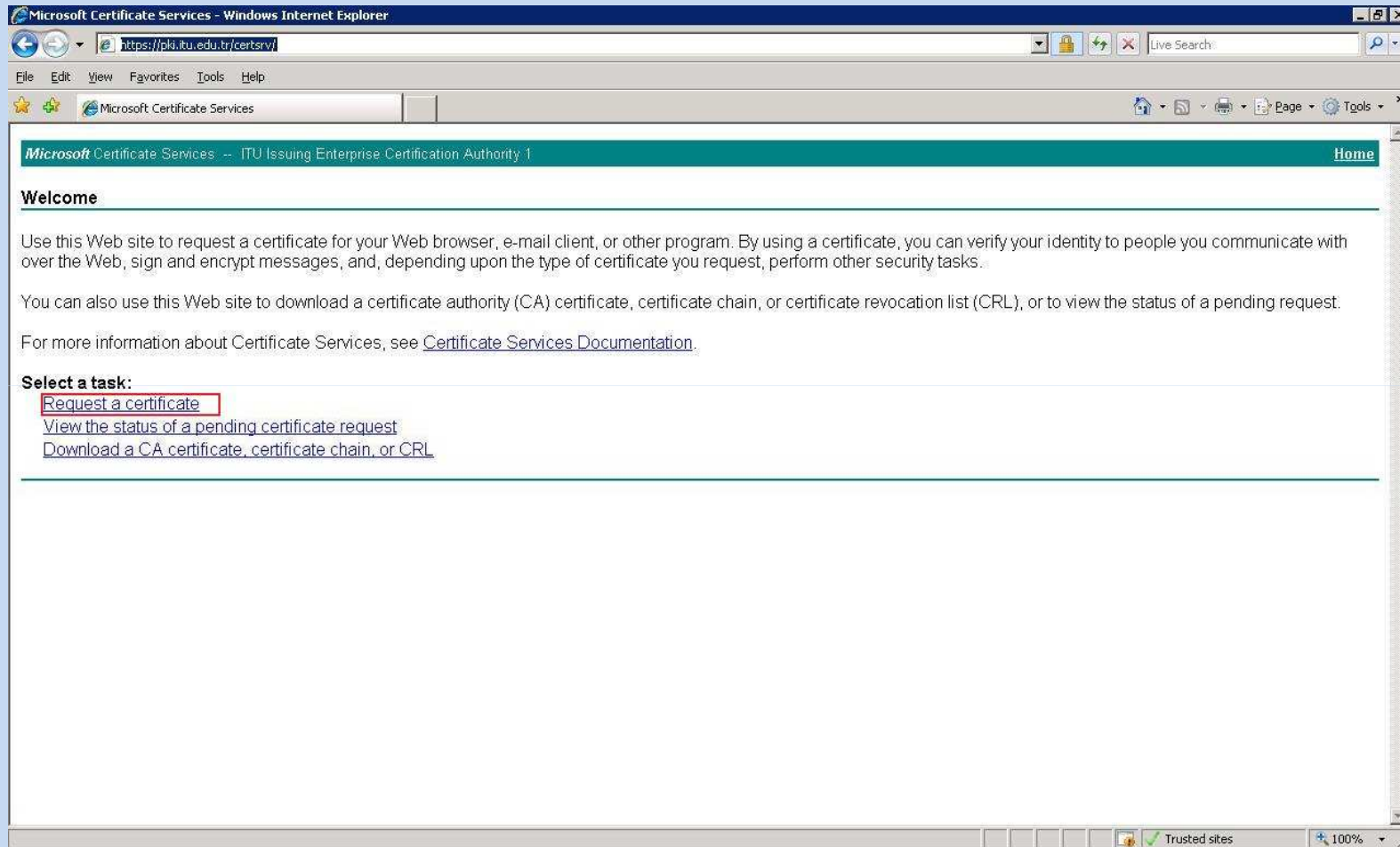
Private key file

Type the full path and file name where you want to store the private key file.

Kök Sertifika ile İmzalatılması (1)

- Bir önceki slaytta kırmızı ile gösterilmiş kısım kopyalanır ve sertifika sunucusunda ilerki slaytlarda işaretlenmiş olan yere yapıştırılır.
- Daha sonra istek sistem destek çalışanı tarafından onaylanır ve pending cert req. Altından onaylama işlemi sonrası sunucuya indirilir.

Kök Sertifika ile İmzalatılması (2)



Kök Sertifika ile İmzalatılması (3)

Microsoft Certificate Services - Windows Internet Explorer

https://pki.itu.edu.tr/certsrv/certrqxt.asp

File Edit View Favorites Tools Help

Microsoft Certificate Services

Microsoft Certificate Services -- ITU Issuing Enterprise Certification Authority 1 [Home](#)

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
MIICyjCCAbICAQAwIDEEeMBwGA1UEAxMVcGVhcGFj
IjANBgkqhkiG9w0BAQEFAAOCQA8AMIIBCgKCAQEA
4AHX5Dw+1KSVNXRaR75Nis0nODsI+/OD48t9DyZD
wpeIdXt+Rj4nsq54dv3U+9A9Bqp815Yb31J0wK2M
iWBQEBOz//mmfIyCZRhcwvQxZV0zyE52g46AryoG
kksOTOe/tZAUj4m2rtCOmerSmUC1rdDKd2hJnIQA
```

[Browse for a file to insert.](#)

Certificate Template:

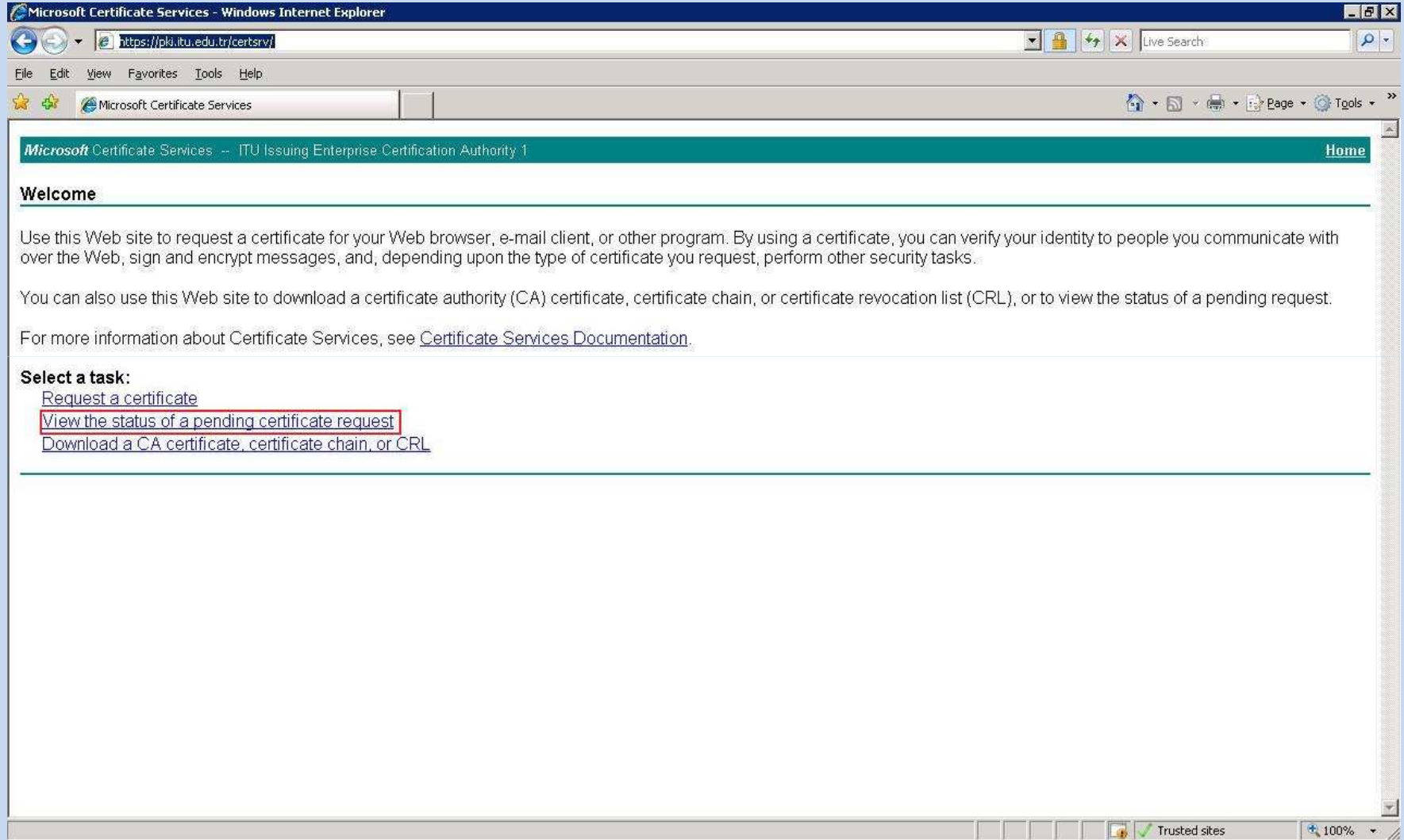
Cisco ACS

Additional Attributes:

Attributes:

Trusted sites 100%

Kök Sertifika ile İmzalatılması (4)



Microsoft Certificate Services - Windows Internet Explorer

https://plk.itu.edu.tr/certsrv/

File Edit View Favorites Tools Help

Microsoft Certificate Services

Microsoft Certificate Services - ITU Issuing Enterprise Certification Authority 1 [Home](#)

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

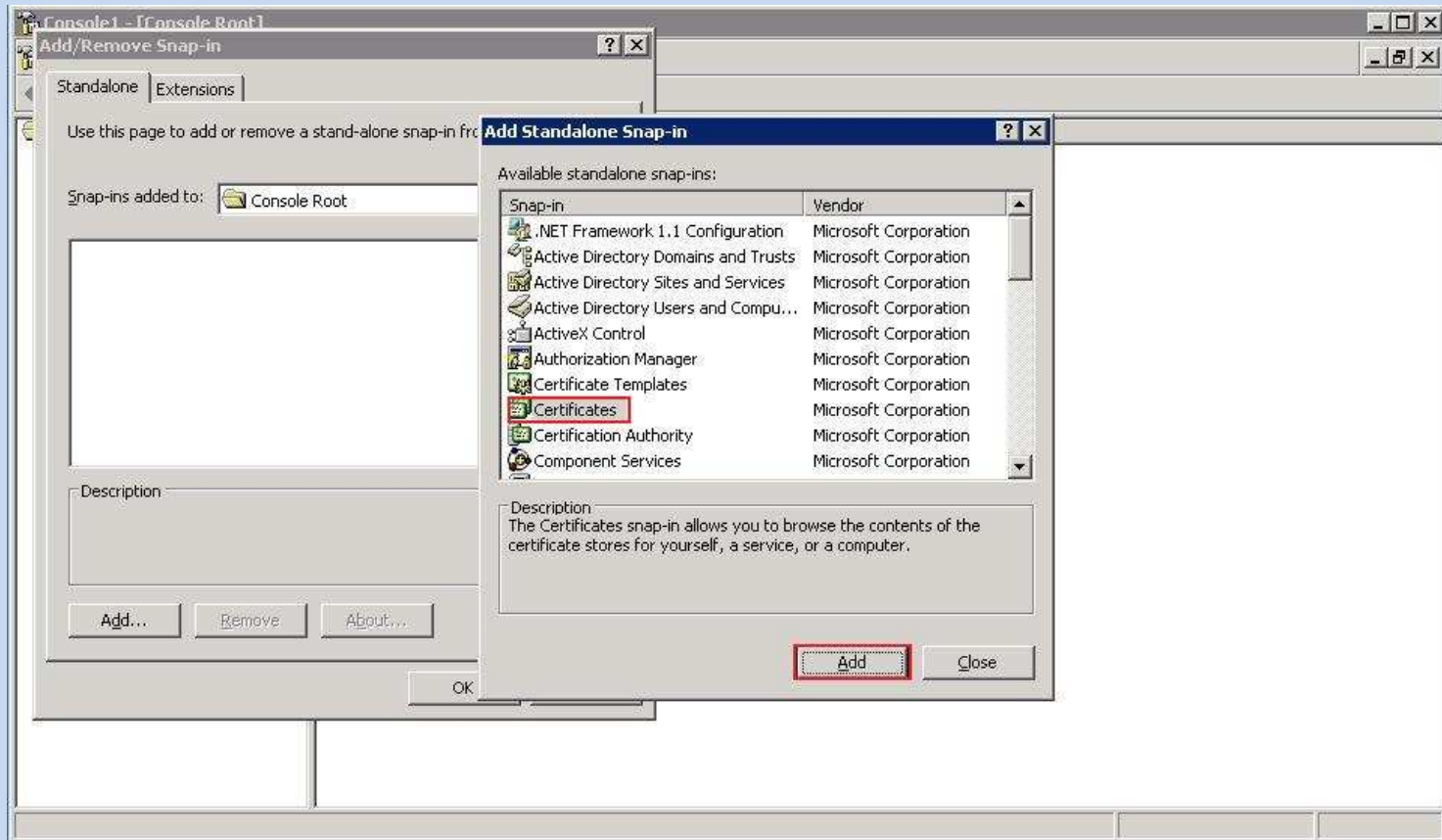
For more information about Certificate Services, see [Certificate Services Documentation](#).

Select a task:

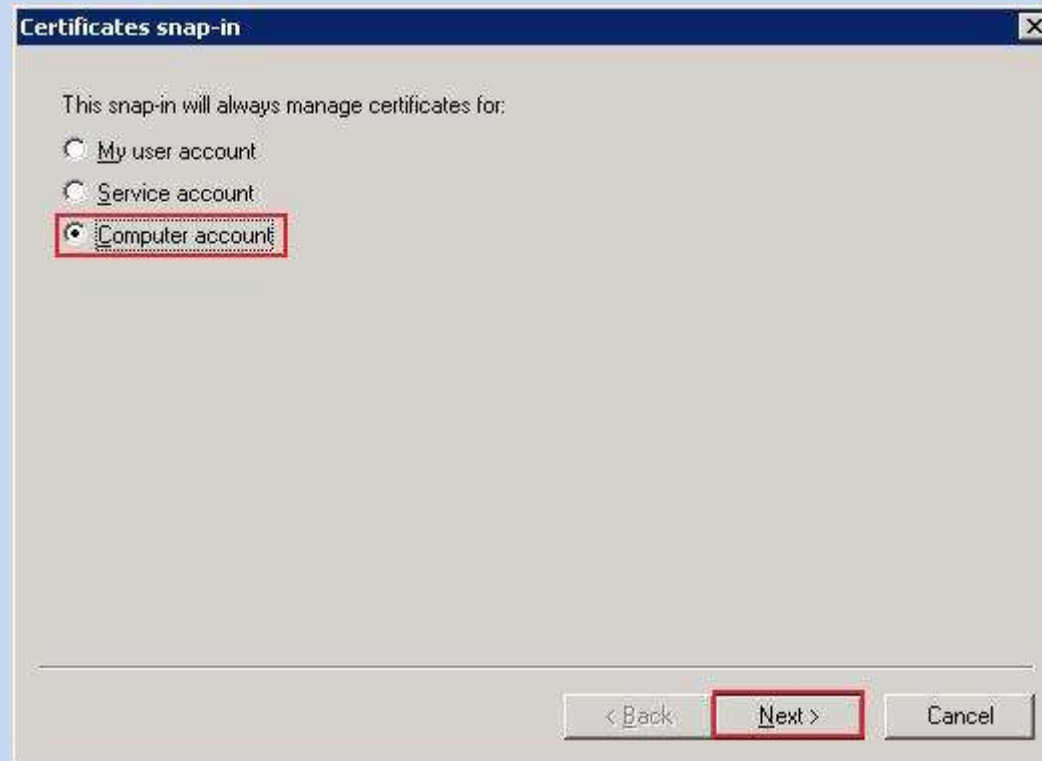
- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

Trusted sites 100%

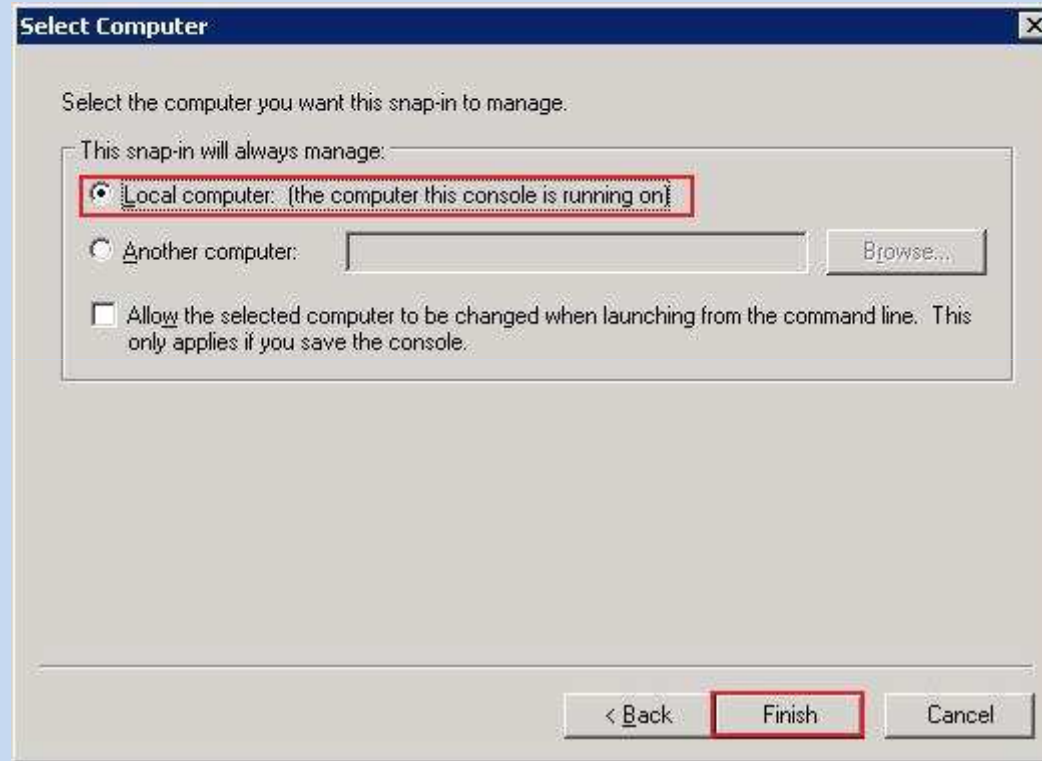
ACS Sunucusuna İmzalanmış Sertifikanın Yüklenmesi(1)



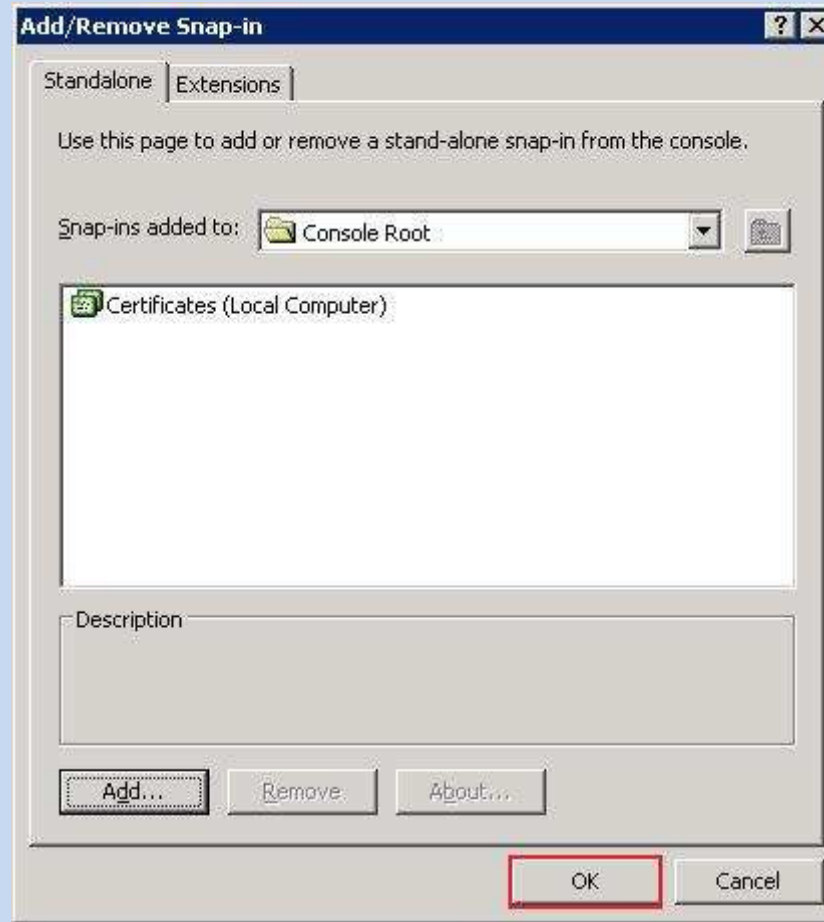
ACS Sunucusuna İmzalanmış Sertifikanın Yüklenmesi(2)



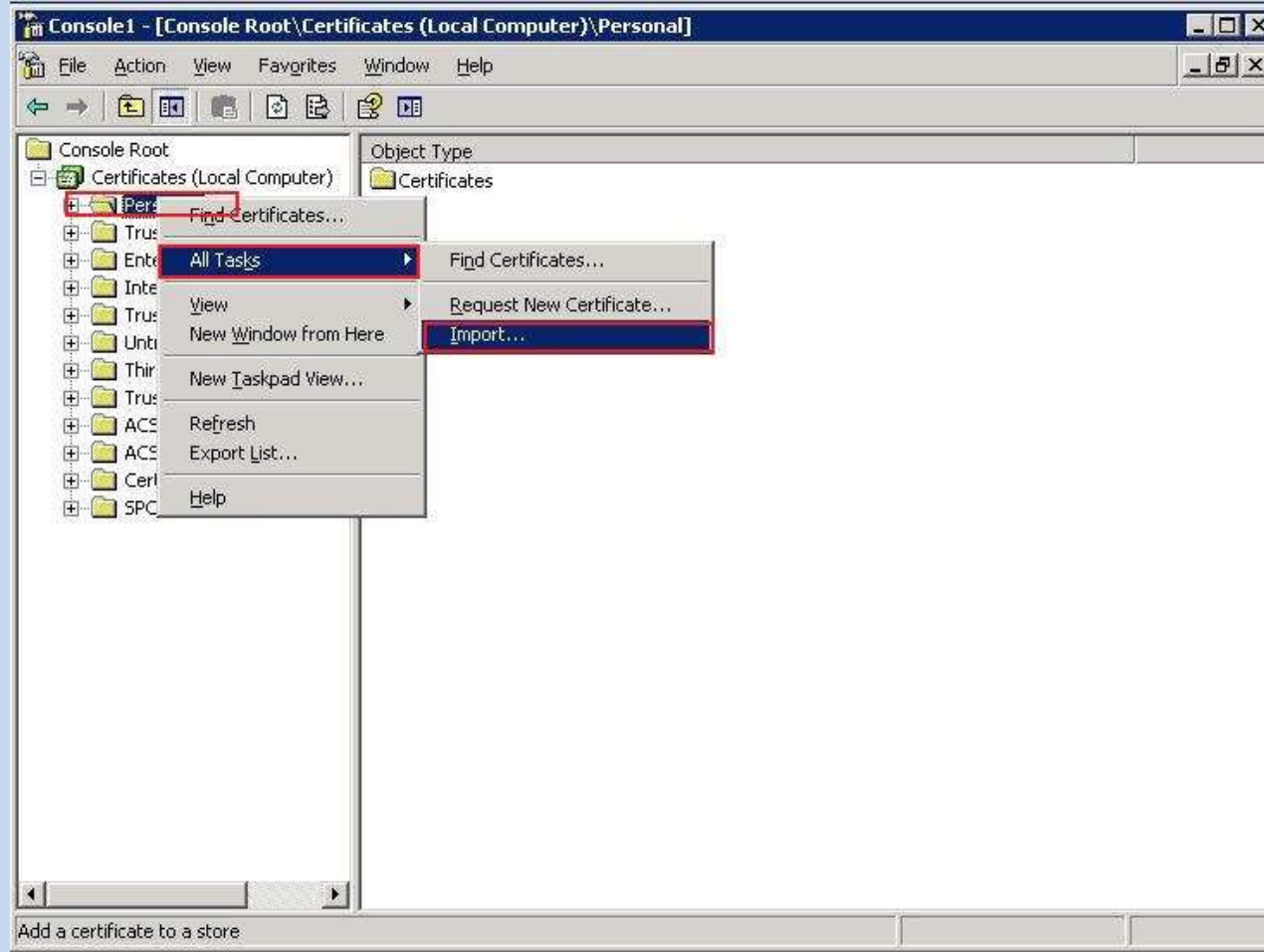
ACS Sunucusuna İmzalanmış Sertifikanın Yüklenmesi(3)



ACS Sunucusuna İmzalanmış Sertifikanın Yüklenmesi(4)



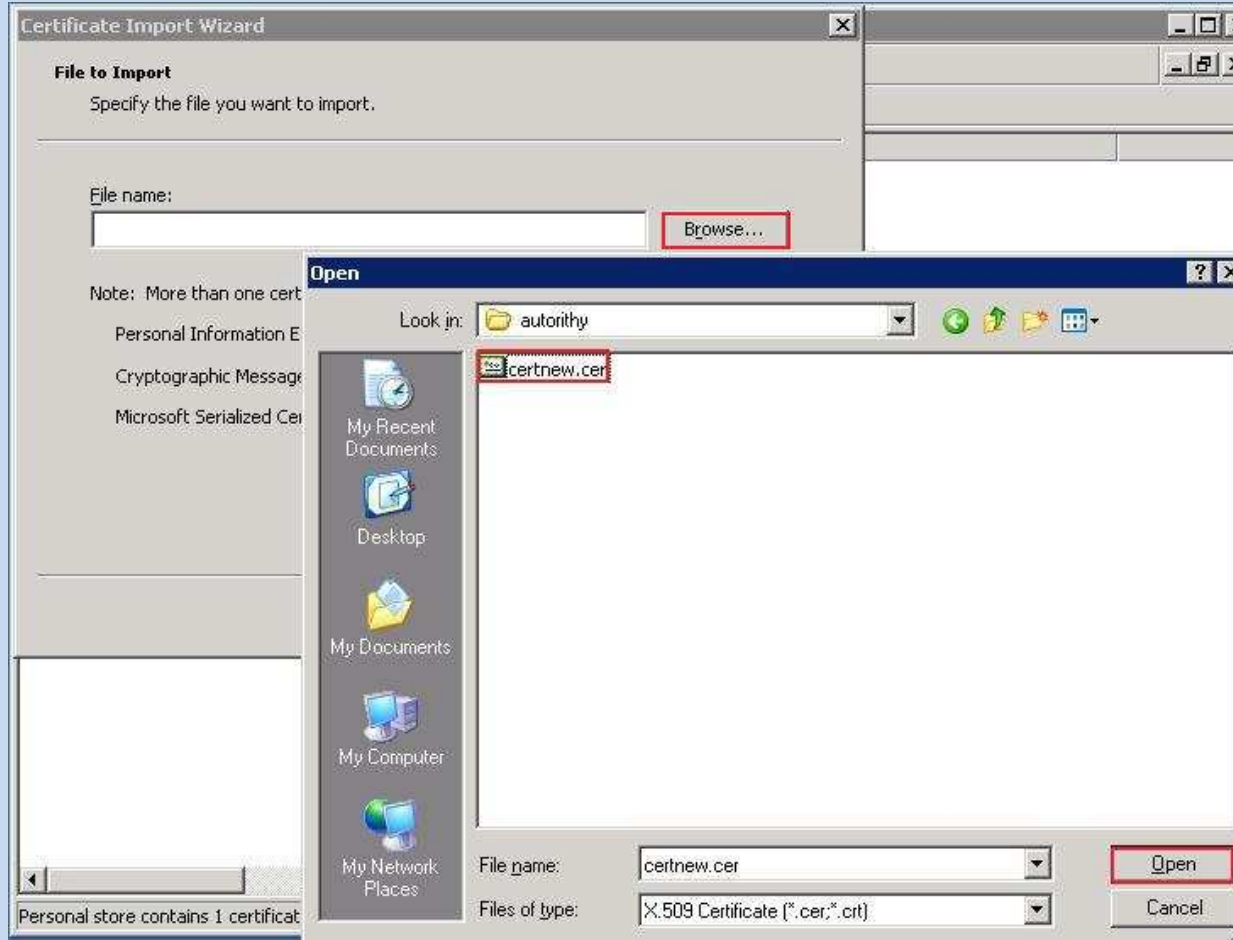
ACS Sunucusuna İmzalanmış Sertifikanın Yüklenmesi(5)



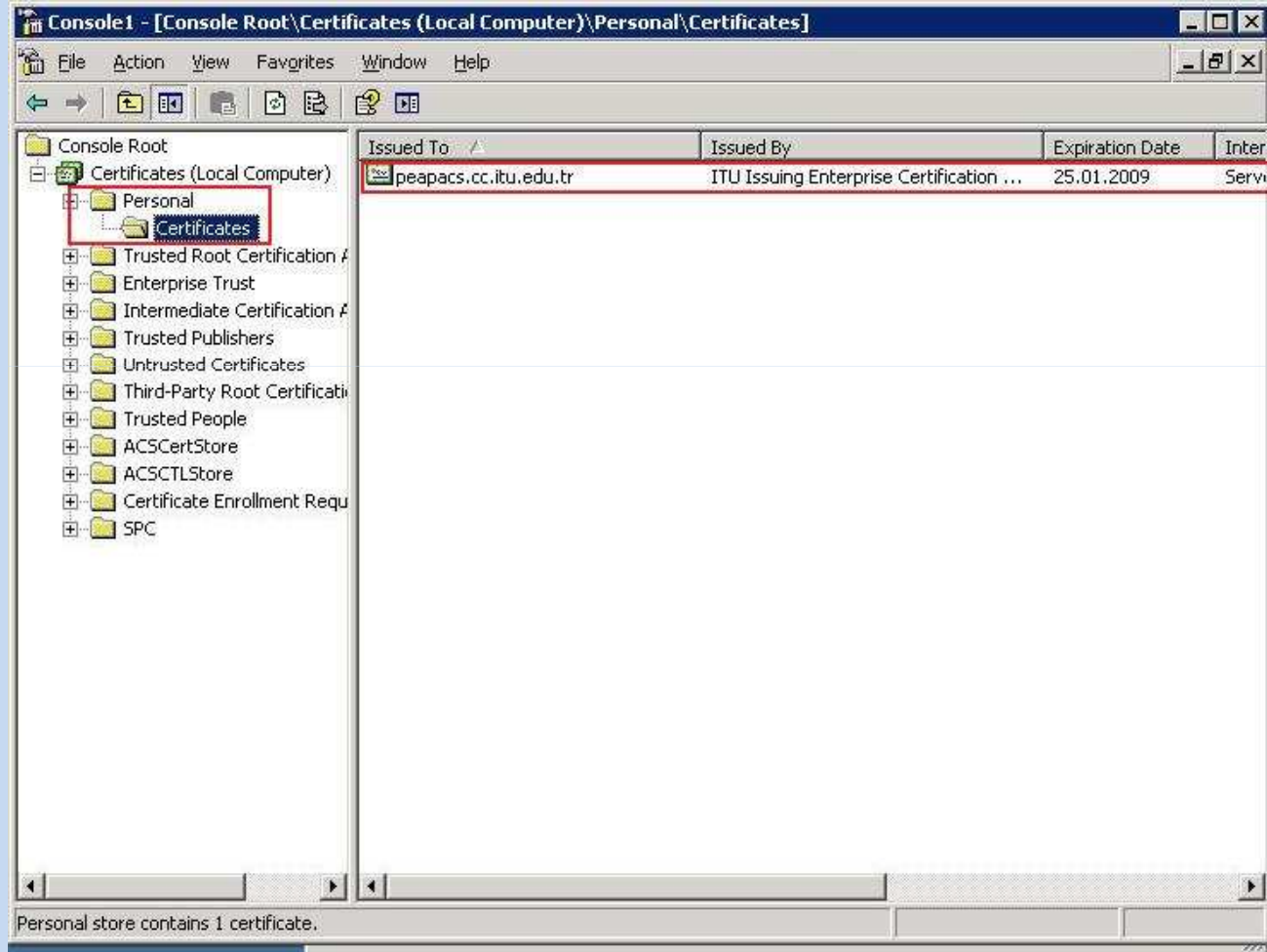
ACS Sunucusuna İmzalanmış Sertifikanın Yüklenmesi(6)



ACS Sunucusuna İmzalanmış Sertifikanın Yüklenmesi(7)



ACS Sunucusuna İmzalanmış Sertifikanın Yüklenmesi(8)



ACS Uygulamasına İmzalanmış Sertifikanın Yüklenmesi(1)

- Daha önceden “c:/key.ini” oluşturmuştuk bunu oluştururken de bir şifre girmiştik bunlar ACS ye gösterilir.
- Sunucu adi CN kısmına yazılır ve submit denir.
- İşlem sonrası ACS restart edilir.

ACS Sunucusuna İmzalanmış Sertifikanın Yüklenmesi(2)

The screenshot displays the CiscoSecure ACS System Configuration web interface. The main content area is titled "Install ACS Certificate" and contains a form for installing a new certificate. The form has two radio buttons: "Read certificate from file" (unselected) and "Use certificate from storage" (selected). The "Use certificate from storage" option is highlighted with a red box. Below this, there are three text input fields, each also highlighted with a red box: "Certificate file" (empty), "Certificate CN" (peapacs.cc.itu.edu.tr), and "Private key file" (c:\key.ini). Below these fields is a "Private key password" field with a masked password (represented by dots). A "Back to Help" button is located below the form. At the bottom of the form are "Submit" and "Cancel" buttons.

The left sidebar contains a navigation menu with the following items: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation.

The right sidebar contains a "Help" section with a list of links: Read certificate from file, Certificate file, Use certificate from storage, Certificate CN, Private key file, and Private key password. Below the links is a paragraph of text: "You can use this page to perform certificate enrollment to support EAP-TLS and PEAP authentication and HTTPS for access to the ACS web interface. ACS supports the X.509 v3 digital certificate standard. Certificate and CA files must be either in Base64-encoded X.509 format or DER-encoded binary X.509 format." Below this is a "Note" section: "Note: Whenever you install a new certificate, you must configure the Certificate Trust List. Replacing an existing certificate configuration with a new certificate configuration automatically erases the previous configuration of the Certificate Trust List." Below the note are three sections: "Read certificate from file" (with a "Back to Top" link), "Certificate file" (with a "Back to Top" link), and "Use certificate from storage" (with a "Back to Top" link).

The browser window title is "CiscoSecure ACS - Windows Internet Explorer" and the address bar shows "http://160.75.5.241:3040/index2.htm". The browser's address bar also shows "CiscoSecure ACS" and "Araçlar". The status bar at the bottom shows "Internet | Korumalı Mod: Kapalı" and "%100".

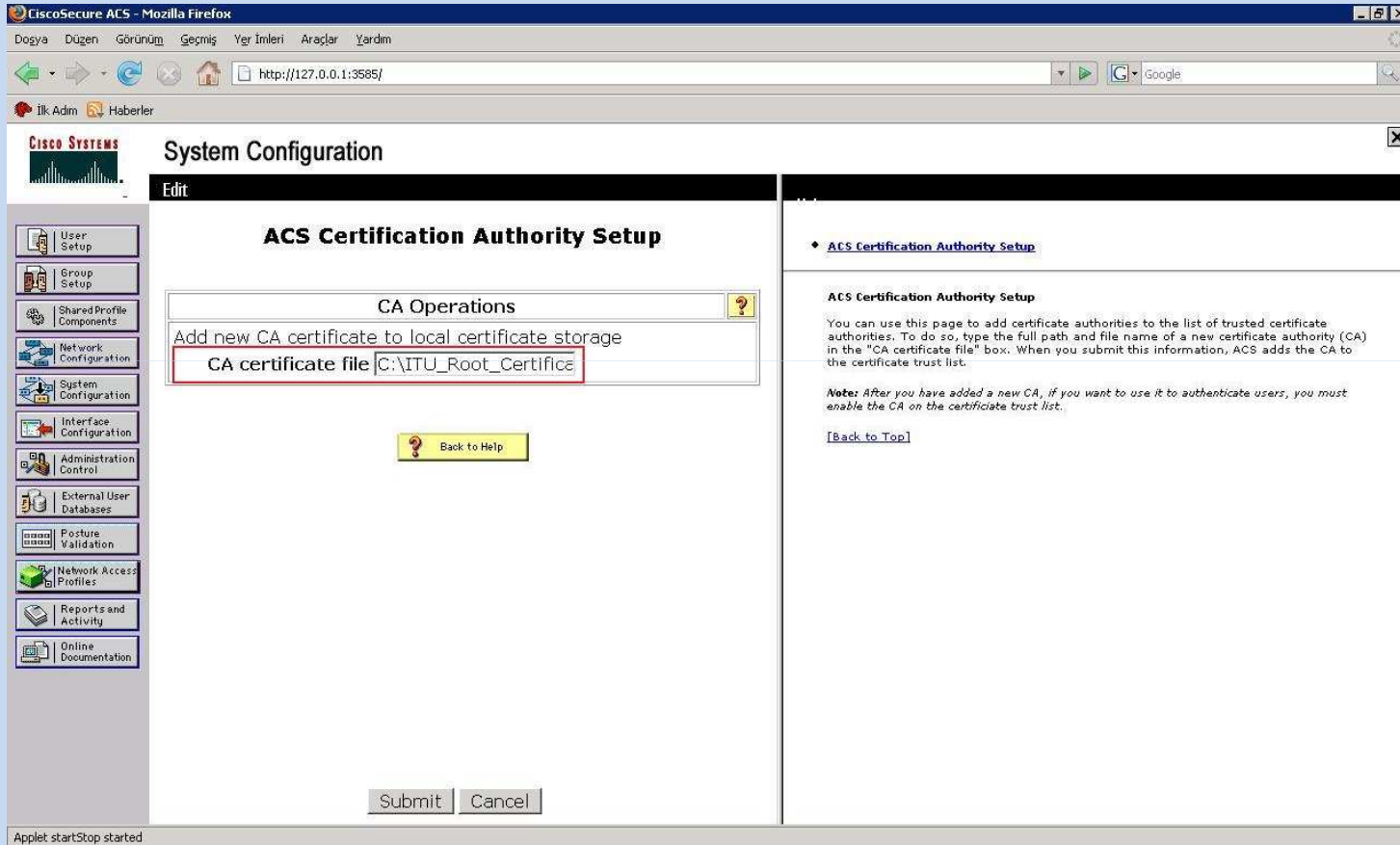
Kök Sertifikanın ACS'ye Kurulumu (1)

- Kök sertifika sunucuya indirilir.
- ACS'ye kök sertifikanın yeri gösterilir.
- İşlem sonrası ACS tekrar başlatılır.
- Bu sertifikanın ekstra Windows'a yüklenmesine gerek yoktur.

Kök Sertifikanın ACS'ye Kurulumu (2)

The screenshot displays the CiscoSecure ACS web interface in Mozilla Firefox. The browser address bar shows the URL <http://127.0.0.1:3585/>. The page title is "System Configuration". The left sidebar contains a navigation menu with the following items: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main content area is titled "ACS Certificate Setup" and lists the following options: [Install ACS Certificate](#), [ACS Certification Authority Setup](#), [Edit Certificate Trust List](#), [Certificate Revocation Lists](#), [Generate Certificate Signing Request](#), and [Generate Self-Signed Certificate](#). A "Cancel" button is located below the list. A yellow "Back to Help" button is also present. On the right side, there is a detailed description for each option, including "Install ACS Certificate", "ACS Certification Authority Setup", "Edit Certificate Trust List", "Certificate Revocation Lists", and "Generate Certificate Signing Request". The "Install ACS Certificate" section includes the text: "Select to install a certificate from Windows certificate storage or from a file." and a "[Back to Top]" link. The "ACS Certification Authority Setup" section includes the text: "Select to add a third-party CA certificate into the ACS CA certificates list." and a "[Back to Top]" link. The "Edit Certificate Trust List" section includes the text: "You can specify which third-party certificate authorities (CAs) ACS should trust when authenticating users with certificate-based protocol. If a user's certificate is from a CA that you have not specifically configured ACS to trust, authentication fails." and a "[Back to Top]" link. The "Certificate Revocation Lists" section includes the text: "You can configure ACS to retrieve certificate revocation lists (CRLs) from CAs that are enabled on the Certificate Trust List." and a "[Back to Top]" link. The "Generate Certificate Signing Request" section includes the text: "You can use ACS to generate a certificate signing request (CSR). Once you have generated a CSR, you can submit it to a certificate authority to receive your certificate." The bottom status bar shows "Tamam".

Kök Sertifikanın ACS'YE Kurulumu (3)



The screenshot shows the CiscoSecure ACS System Configuration interface in a Mozilla Firefox browser. The browser's address bar displays the URL <http://127.0.0.1:3585/>. The page title is "System Configuration" and the current page is "ACS Certification Authority Setup".

The left sidebar contains a navigation menu with the following items:

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

The main content area is titled "ACS Certification Authority Setup" and features a "CA Operations" section. The "Add new CA certificate to local certificate storage" form includes a text input field for the "CA certificate file" with the value "C:\ITU_Root_Certificat". Below the form is a "Back to Help" button. At the bottom of the form are "Submit" and "Cancel" buttons.

The right sidebar contains a section titled "ACS Certification Authority Setup" with the following text:

ACS Certification Authority Setup

You can use this page to add certificate authorities to the list of trusted certificate authorities. To do so, type the full path and file name of a new certificate authority (CA) in the "CA certificate file" box. When you submit this information, ACS adds the CA to the certificate trust list.

Note: After you have added a new CA, if you want to use it to authenticate users, you must enable the CA on the certificate trust list.

[\[Back to Top\]](#)

ACS'de Gereken Kimlik Denetimi Ayarları (1)

The screenshot shows the Cisco ACS System Configuration interface in Mozilla Firefox. The main content area is titled "Global Authentication Setup" and contains an "EAP Configuration" section. In the "PEAP" section, the "Allow EAP-MSCHAPv2" checkbox is checked, while "Allow EAP-GTC" is also checked. The "PEAP session timeout (minutes)" is set to 120. The "EAP-FAST" section is currently empty. The "EAP-TLS" section has "Allow EAP-TLS" unchecked, and the "EAP-TLS session timeout (minutes)" is set to 120. The "Submit + Restart" button is highlighted in red. The right sidebar contains a "Global Authentication Setup" section with a list of links: EAP Configuration, PEAP, EAP-FAST, EAP-TLS, LEAP, EAP-MDS, AP EAP Request Timeout, and MS-CHAP Configuration. Below this is an "EAP Configuration" section with a detailed description of EAP and a list of configuration options: Allow EAP-MSCHAPv2, Allow EAP-GTC, Allow Posture Validation, Cisco client initial message, PEAP session timeout (minutes), and Enable Fast Reconnect.

MSCHAP2 seçeneği işaretlenir ve onaylanır.

Kablosuz Erişim Cihazlarının ACS'ye Tanılması (1)

Network Configuration

Select

AAA Client Hostname	AAA Client IP Address	Authenticate Using
peapap	160.75.5.71	RADIUS (Cisco Aironet)

Add Entry Search

AAA Server Name	AAA Server IP Address	AAA Server Type
peapacs	160.75.2.109	CiscoSecure ACS

Add Entry Search

Character String	AAA Servers	Strip	Account
(Default)	peapacs	No	Local

Add Entry Sort Entries

- Network Device Groups
- Adding a Network Device Group
- Editing a Network Device Group
- Deleting a Network Device Group
- Searching for Network Devices
- AAA Clients
- Adding a AAA Client
- Editing a AAA Client
- Deleting a AAA Client
- AAA Servers
- Adding a AAA Server
- Editing a AAA Server
- Deleting a AAA Server
- Proxy Distribution Table
- Adding a Proxy Distribution Table Entry
- Sorting Proxy Distribution Table Entries
- Editing a Proxy Distribution Table Entry
- Deleting a Proxy Distribution Table Entry

Note: This page changes depending your interface configuration. If you are using Network Device Groups (NDGs), after you click Network Configuration in the navigation bar, only the Network Device Groups table and Proxy Distribution Table information appear. If you are not using NDGs, the AAA Clients table and the AAA Servers table appear in place of the Network Device Groups table.

Network Device Groups

Network device groups are collections of AAA clients and AAA servers. You can assign AAA clients and AAA servers to the network device groups you create. AAA clients and AAA servers not assigned to a particular NDG are, by default, assigned to the Not Assigned NDG.

To view the AAA Client and AAA Servers tables for a particular NDG, click the name of the NDG.

[Back to Top]

Adding a Network Device Group

To add an NDG to the list, click **Add Entry**, directly under the **Network Device Groups** table.

ACS'yi kullanacağımız cihazlar IP adresi ve anahtar kelime ile tanılır. Anahtar kelimenin aynısı kablosuz erişim cihazlarında da tanıtılmalıdır.

Kablosuz Erişim Cihazlarının ACS'ye Tanıtılması (2)

The screenshot displays the CiscoSecure ACS web interface in Mozilla Firefox. The browser address bar shows the URL <http://127.0.0.1:3585/>. The page title is "Network Configuration" and the sub-page is "Edit". The main content area is titled "Add AAA Client" and contains the following form fields and options:

- AAA Client Hostname:
- AAA Client IP Address:
- Key:
- Authenticate Using:
- Single Connect TACACS+ AAA Client (Record stop in accounting on failure).
- Log Update/Watchdog Packets from this AAA Client
- Log RADIUS Tunneling Packets from this AAA Client
- Replace RADIUS Port info with Username from this AAA Client

At the bottom of the form, there are three buttons: "Submit", "Submit + Apply" (highlighted with a red box), and "Cancel". Below these buttons is a "Back to Help" button with a question mark icon.

On the right side of the page, there is a list of configuration options for the AAA Client:

- [AAA Client Hostname](#)
- [AAA Client IP Address](#)
- [Key](#)
- [Network Device Group](#)
- [Authenticate Using](#)
- [Single Connect TACACS+ AAA Client](#)
- [Log Update/Watchdog Packets from this AAA Client](#)
- [Log RADIUS Tunneling Packets from this AAA Client](#)
- [Replace RADIUS Port info with Username from this AAA Client](#)

Below this list, there are two sections of explanatory text:

AAA Client Hostname
The AAA Client Hostname is the name assigned to the AAA client.
[\[Back to Top\]](#)

AAA Client IP Address
The AAA Client IP Address is the IP address assigned to the AAA client.
If you want to designate more than one AAA client with a single AAA client entry in ACS, you can specify the IP address for each AAA client to be represented by this AAA client entry. To separate each IP address, press **Enter**.
You can use the wildcard asterisk (*) for an octet in the IP address. For example, if you want every AAA client in your 192.168.13.1 Class C network to be represented by a single AAA client entry, enter 192.168.13.* in the AAA Client IP Address box.
You can define ranges within an octet of an IP address. For example, if you want every AAA client with an IP address between 192.168.13.12 and 192.168.13.221 to be represented by a single AAA client entry, enter 192.168.13.12-221 in the AAA Client IP Address box.
[\[Back to Top\]](#)

Key
The Key is the shared secret that the TACACS+ or RADIUS AAA client and ACS use to encrypt the data. The key must be configured in the AAA client and ACS identically, including case sensitivity.

Ekstra Notlar

- Sunucunun IP adresi deđiştirilirse ACS ve sunucu tekrar başlatılmalıdır.
- Sunucunun DNS kaydının olmaması herhangi bir sorun yaratmaz.
- Kök sertifikasının ayrıca Windows'a yüklenmesine gerek yoktur.

ACS'nin Active Directory Üzerinde Kimlik Denetimi Yapması (1)

The screenshot displays the CiscoSecure ACS web interface in a Mozilla Firefox browser window. The browser's address bar shows the URL <http://127.0.0.1:3585/>. The page title is "External User Databases". On the left side, there is a navigation menu with various configuration options, including "External User Databases" which is highlighted with a red box. The main content area is divided into two columns. The left column, titled "Select", contains three links: "Unknown User Policy", "Database Group Mappings", and "Database Configuration", with the latter being highlighted by a red box. Below these links is a "Back to Help" button. The right column contains a list of links: "Unknown User Policy", "Database Group Mappings", and "Database Configuration", each followed by a brief description and a "[Back to Top]" link. The "Database Configuration" link is highlighted with a red box. The bottom of the page shows the status "Tamam".

CiscoSecure ACS - Mozilla Firefox

Doğya Düzen Görünüm Geçmiş Yer İmleri Araçlar Yardım

<http://127.0.0.1:3585/> Google

İlk Adım Haberler

CISCO SYSTEMS External User Databases

Select

- Unknown User Policy
- Database Group Mappings
- Database Configuration

Back to Help

- Unknown User Policy
- Database Group Mappings
- Database Configuration

Unknown User Policy
Click to configure the authentication procedure for unknown users not configured in the ACS internal database.
[\[Back to Top\]](#)

Database Group Mappings
Click to configure the ACS group authorization privileges that unknown users who authenticate to an external database will inherit.
[\[Back to Top\]](#)

Database Configuration
Click to configure a particular external database type for users to authenticate against. ACS can authenticate users with the Windows user database as well as with token servers and other supported third-party databases.
[\[Back to Top\]](#)

Tamam

ACS'nin Active Directory Üzerinde Kimlik Denetimi Yapması (2)

CiscoSecure ACS - Mozilla Firefox

http://127.0.0.1:3585/

External User Databases

Select

External User Database Configuration

Choose which external user database type to configure.

- Windows Database**
- Generic LDAP
- External ODBC Database
- LEAP Proxy RADIUS Server
- RADIUS Token Server
- RSA SecurID Token Server

[List all database configurations](#)

Cancel

Back to Help

- Windows Database**
Click to configure Windows SAM and Active Directory databases with which ACS can authenticate users.
[\[Back to Top\]](#)
- Generic LDAP**
Click to add or configure a generic LDAP datasource with which ACS can authenticate users. An example of a generic LDAP datasource is Netscape Directory Service. While Active Directory is based on LDAP, use a Windows database configuration for authenticating users with Active Directory.
[\[Back to Top\]](#)
- External ODBC Database**
Click to add or configure an Open DataBase Connectivity (ODBC) datasource with which ACS can authenticate users.
[\[Back to Top\]](#)
- LEAP Proxy RADIUS Server**
Click to add or configure a LEAP Proxy RADIUS Server external user database with which ACS can authenticate users.
[\[Back to Top\]](#)
- Token Card Server Support**

Tamam

ACS'nin Active Directory Üzerinde Kimlik Denetimi Yapması (3)

CiscoSecure ACS - Mozilla Firefox

Doğya Düzen Görünüm Geçmiş Yer İmleri Araçlar Yardım

http://127.0.0.1:3585/

Ilk Adım Haberler

External User Databases

Edit

External User Database Configuration

Choose what to do with the Windows Database database.

[Configure](#) [Delete](#)

[Cancel](#)

[Back to Help](#)

- ◆ [Windows Database](#)
- ◆ [Generic LDAP](#)
- ◆ [External ODBC Database](#)
- ◆ [LEAP Proxy RADIUS Server](#)
- ◆ [Token Card Server Support](#)
- ◆ [RADIUS Token Server](#)
- ◆ [RSA SecurIDToken Server](#)

Windows Database

Click to configure Windows SAM and Active Directory databases with which ACS can authenticate users.

[\[Back to Top\]](#)

Generic LDAP

Click to add or configure a generic LDAP datasource with which ACS can authenticate users. An example of a generic LDAP datasource is Netscape Directory Service. While Active Directory is based on LDAP, use a [Windows](#) database configuration for authenticating users with Active Directory.

[\[Back to Top\]](#)

External ODBC Database

Click to add or configure an Open DataBase Connectivity (ODBC) datasource with which ACS can authenticate users.

[\[Back to Top\]](#)

LEAP Proxy RADIUS Server

Click to add or configure a LEAP Proxy RADIUS Server external user database with which ACS can authenticate users.

[\[Back to Top\]](#)

Token Card Server Support

Tamam

ACS'nin Active Directory Üzerinde Kimlik Denetimi Yapması (4)

database on the Selected Databases list, you may enable this option.

Configure Domain List

Available Domains	Domain List
LOCAL	ITU
CC	
CMI	
IDARI	
LABS	
REKTORLUK	

Up Down

MS-CHAP Settings

Enable password changes using MS-CHAP version 1.

Applet selectUserGroups started

- Windows Database Configuration
- Dialin Permission
- Windows Callback
- Unknown User Policy
- Configure Domain List
- MS-CHAP Settings
- Windows EAP Settings

Windows Database Configuration

Configure your Windows database. ACS supports Windows SAM and Active Directory user databases.

Dialin Permission

When this feature is enabled, users must have dialin permission in order to authenticate. If you did not already do so during installation, enable your ACS to grant dialin permission to users by selecting the top check box. The Microsoft Windows domain must also be configured to allow grant dialin permission to user. See your Microsoft documentation for more information.

[\[Back to Top\]](#)

Windows Callback

You should enable this setting if you have Windows users that require dialup access with callback and the User Setup or Group Setup callback setting is configured for Windows Database Callback. If dialup access with callback is not required or is not configured for Windows Database Callback, then do not enable this setting.

[\[Back to Top\]](#)

Unknown User Policy

If a user does not exist in the Windows database, or has typed an incorrect password, the following error "**1326(bad username or password)**" is returned. ACS treats this error as a "wrong password" error and does not search other external databases. This option should be enabled when there are additional external databases listed after the Windows database in the Selected Databases list. When enabled, ACS searches for the unknown user in the other external databases.

Kimlik denetimi yapılacak domain seçilir ve uygulanır.

Teşekkürler

İTÜ/BİDB 2008