

Locally Significant Certificates on Wireless LAN Controllers Configuration Example

Document ID: 110141

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Locally Significant Certificates

- Certificate Provisioning on Wireless LAN Controllers (WLCs)
- Certificate Provisioning on LWAPP AP
- LSC Support on Wireless LAN Controllers (WLCs) and Lightweight Access Points (LAPs)

Configure

- Network Setup
- Configure the Wireless LAN Controller through the GUI
- Configure the Wireless LAN Controller through the CLI

Verify

Troubleshoot

Related Information

Introduction

This document explains how to configure the Wireless LAN Controller (WLC) and Lightweight Access Points to use the Locally Significant Certificate feature. This feature is introduced with Wireless LAN Controller Version 5.2. With this feature, if you choose to control public key infrastructure (PKI), you can generate locally significant certificates (LSC) on the access points and controllers. These certificates can then be used to mutually authenticate the Wireless LAN Controller (WLC) and Lightweight Access Point (LAP).

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Knowledge of how to configure the WLC, lightweight access point (LAP), and wireless client card for basic operation
- Knowledge of how to configure and use the Microsoft Windows 2003 CA server
- Knowledge of Public key infrastructure and digital certificates

Components Used

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

- Cisco 4400 Series WLC that runs firmware 5.2
- Cisco Aironet 1130 AG Series Lightweight Access Point (LAP)
- Microsoft Windows 2003 server configured as domain controller, and as a Certificate Authority server.

- Cisco Aironet 802.11 a/b/g Client Adapter that runs firmware release 4.2
- Cisco Aironet Desktop Utility (ADU) that runs firmware version 4.2

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 Cisco Technical Tips Conventions for more information on document conventions.

Locally Significant Certificates

In controller software releases earlier than 5.2.157.0, the controller can either use self-signed certificates (SSCs) to authenticate access points or send the authorization information to a RADIUS server, if access points have manufacturing-installed certificates (MICs). In controller software release 5.2.157.0, you can configure the controller to use a local significant certificate (LSC). You can use an LSC if you want your own public key infrastructure (PKI) to provide better security; to have control of your certificate authority (CA), and to define policies, restrictions, and usages on the generated certificates.

The new LSC certificates needs to be provisioned on the Controller first and then the LAP from the Certificate Authority (CA) Server.

The LAP communicates with the Controller (WLC) with the CAPWAP protocol. Any requests to sign the certificate and issue the CA certificates for the LAP and for the WLC itself, must be initiated from the WLC. The LAP does not communicate directly with the CA Server. The WLC behaves as a CA-proxy to the AP of the LWAPP. The CA Server details must be configured on the WLC, and it must be reachable.

The Controller makes use of the Simple Certificate Enrollment Protocol (SCEP) to forward the certReqs generated on the devices to the CA and makes use of SCEP again to get the signed certificates from the CA.

SCEP is a certificate management protocol that Public Key Infrastructure (PKI) clients and Certificate Authority servers use to support certificate enrollment and revocation. It is widely used in Cisco and supported by many CA-Servers. In the SCEP protocol, HTTP is used as the transport protocol for the PKI messages. The primary goal of SCEP is the secure issuance of certificates to network devices. SCEP is capable of many operations, but for this project and release, SCEP is utilized for these operations.

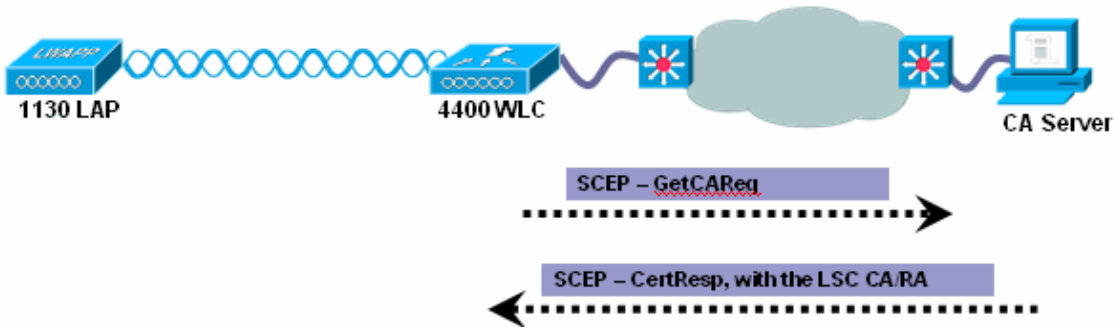
- CA and RA Public Key Distribution
- Certificate Enrollment

All SCEP transactions happen in automatic mode. Certificate Revocation is not supported.

Certificate Provisioning on Wireless LAN Controllers (WLCs)

The new LSC certificates, both the CA and the Device certificates must be installed on the Controller.

With the SCEP protocol, the CA certificates are received from the CA Server. Since at this point, there are no certificates present on the controller, this operation is a clear Get Operation. These are installed on the Controller. These same CA certificates are also pushed to the APs when the APs are provisioned with LSCs.



Device Certificate Enrollment Operation

For both the LAP and the Controller that requests a CA signed certificate, the certRequest is sent as a PKCS#10 message. The certRequest contains the Subject Name, PublicKey and other attributes to be included in the X.509 certificate, and digitally signed by the PrivateKey of the Requester. These must be sent to the CA, which transforms the certRequest into an X.509 certificate.

The CA that receives a PKCS#10 certRequest requires additional information to authenticate the requester identity and verify that the request is unaltered. Many times PKCS#10 combined with other approaches, such as PKCS#7, to send and receive the Cert Reqs/Resps.

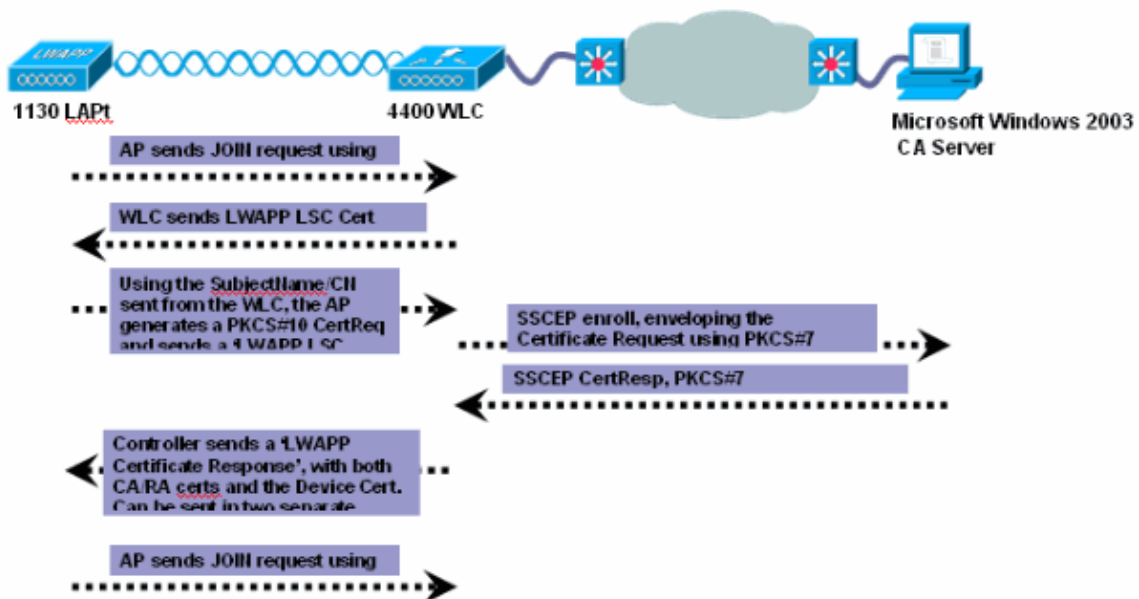
Here, the the PKCS#10 is wrapped in a PKCS#7 SignedData message type. This is supported as part of the SCEP client functionality, while the PKCSReq message is sent to the Controller.

Upon successful enrollment operation, both the CA and Device certificate are now present on the Controller.

Certificate Provisioning on LWAPP AP

In order for a new Certificate to be provisioned on the LAP, while in CAPWAP mode the LAP must be able to get the new signed X.509 certificate. In order to do this, it sends a certRequest to the Controller, which acts as a CA-proxy and helps obtain the certRequest signed by the CA for the LAP.

The certReq and the certResponses are sent to the LAP with the LWAPP payloads. This diagram shows the flow for LAP to provision an LSC.



Here are the steps in detail:

1. The provisioning of the LAP with newer LSCs happens once the LAP is in UP state, after it has JOINED the WLC with its current MIC/SSC. In LSC Provisioning phase, even though the AP is in UP State, the radios are forcibly shut down.
2. The use and provision of the LSC must be enabled on the WLC. This process includes to enable LSC, add CA Server, and configure other Parameters. A LSC Certificate Parameters Command Request is sent from the Controller to LAP, with the subject-name, Validity Time and Keysize set in the payload. These fields are used by the LAP when the certRequest is created. The payload also indicates that the LAP must create a certRequest and send it back to the Controller.
3. The LAP generates the configured keysize public/private RSA key pair. After the generation of the keypair, a certRequest is generated after the SubjectName received from the Controller is configured. The CN is autogenerated with the existing SSC/MIC format, Cxxxx-EtherMacAddr . The LAP generates a PKCS#10 CertReq and sends it as a payload, LSC Certificate Request, to the Controller.
4. The Controller then creates a SSCEP PKCSReq message, a PKCS#7 formatted message, and sends it to the CA on behalf of the :LAP, in order to get the certificate request signed by the configured CA. The installed CA/RA certs are used to encrypt the certReq.
5. If CA is able to approve the Certificate request, a CertRep message with Status=SUCCESS is sent back to the SSCEP client (controller) in a PKCS#7 format. The Cert Response is written locally into a file as a PEM format certificate.
6. Since this CertResp is for the LAP, WLC sends the certificate to the LAP with a payload Certificate Response . The CA cert is sent first with the same payload, then the Device certificate is sent in a separate payload.

Both the LSC CA and the LAP Device certificates are installed into the LAP, and the system self-reboots. The next time it comes up, since it is configured to use LSCs, the AP sends the LSC Device Certificate to the Controller as part of the JOIN Request. As part of the JOIN Response, the controller sends its new Device certificate and also validates the inbound LAP certificate with the new CA Root Certificate.

Note: LSCs are not supported on access points that are configured for bridge mode.

LSC Support on Wireless LAN Controllers (WLCs) and Lightweight Access Points (LAPs)

LSC is supported on these WLC Platforms:

- Cisco 4400 Series Wireless LAN Controllers
- Cisco 2100 Series Wireless LAN Controllers
- Cisco Catalyst 6500 Series Wireless Services Module (WiSM)
- Cisco Catalyst 3750G Integrated Wireless LAN Controller
- Cisco Wireless LAN Controller Module

LSC is supported on Cisco Aironet C1130, C1140, C1240, C1252 Access Points and any new Access Points.

LSC is not supported on MESH AP (1510, 1522), Bridge Mode AP.

This document explains with a configuration example, how to enable and authenticate LAPs with the Locally Significant Certificates.

Configure

Note: The document assumes that the CA server configuration on the Microsoft Windows 2003 server is in place. This document covers the configuration required on the Wireless LAN controller in order to enable this

feature.

The Locally Significant Certificate feature can be enabled through the GUI or the CLI on the controller.

Network Setup

In this example, you configure a 4400 Wireless LAN controller and 1130 series Lightweight Access Point to use the locally significant certificates (LSCs). In order to accomplish this, you must provision the Wireless LAN Controller and the LAP with LSCs from the Certificate Authority (CA) server.

This document uses the Microsoft Windows 2003 server as the CA server.

Configure the Wireless LAN Controller through the GUI

Complete these steps:

1. From the Wireless LAN Controller GUI, click **Security > Certificate > LSC** in order to open the Local Significant Certificates (LSC) page.
2. Click the **General** tab.
3. In order to enable LSC on the system, check the **Enable LSC on Controller** check box.
4. In the CA Server URL field, enter the URL to the CA server. You can enter either a domain name or an IP address.
5. In the Params fields, enter the parameters for the device certificate. The key size is a value from 384 to 2048 (in bits), and the default value is 2048.
6. Click **Apply** to commit your changes.

Local Significant Certificates (LSC)

General **AP Provisioning**

Certificate Type	Status
CA	Not Present ▼

General

Enable LSC on Controller

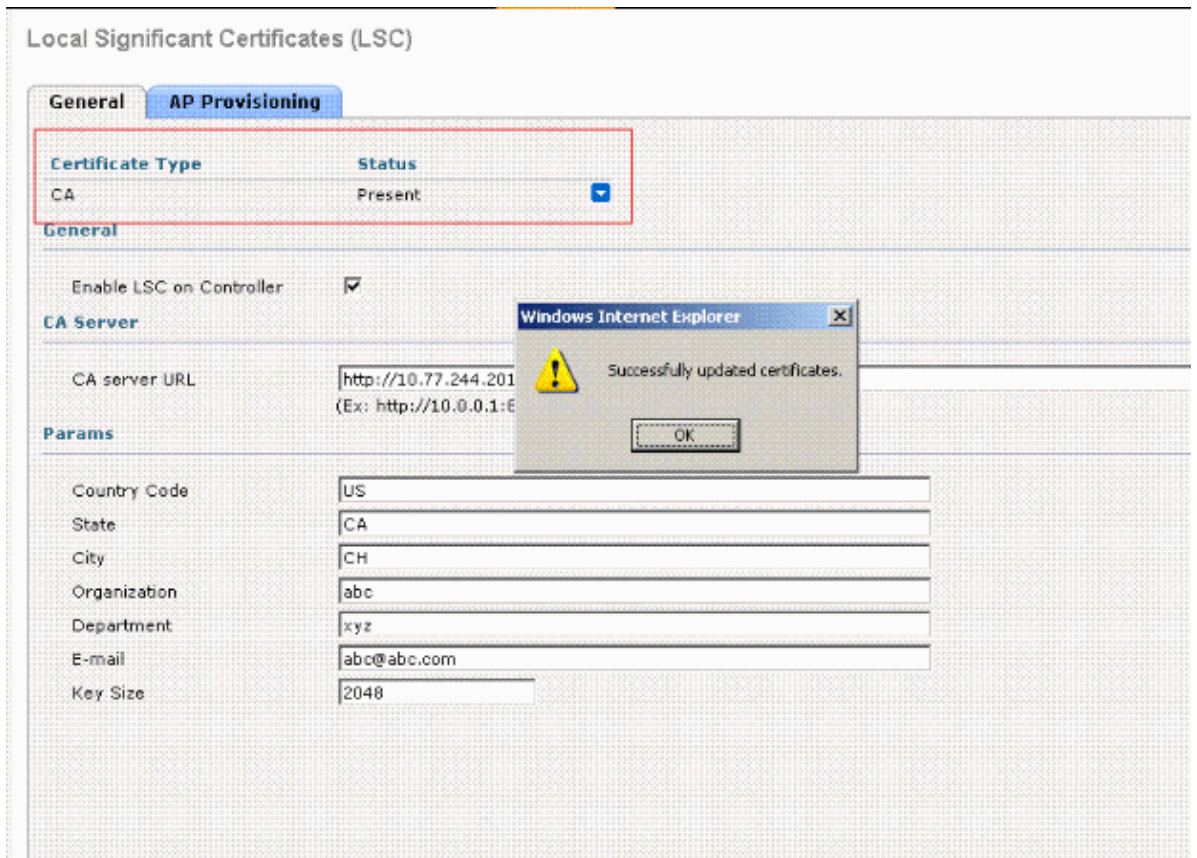
CA Server

CA server URL
(Ex: http://10.0.0.1:8080/caserver)

Params

Country Code	<input type="text" value="US"/>
State	<input type="text" value="CA"/>
City	<input type="text" value="CH"/>
Organization	<input type="text" value="abc"/>
Department	<input type="text" value="xyz"/>
E-mail	<input type="text" value="abc@abc.com"/>
Key Size	<input type="text" value="2048"/>

7. In order to add the CA certificate into the CA certificate database of the controller, hover your cursor over the blue drop-down arrow for the certificate type, and choose **Add**. Here is an example.



8. In order to provision the LSC on the access point, click the **AP Provisioning** tab, and check the **Enable AP Provisioning** check box.
9. In order to add access points to the provision list, enter the access point MAC address in the AP Ethernet MAC Addresses field and click **Add**. In order to remove an access point from the provision list, hover your cursor over the blue drop-down arrow for the access point, and choose **Remove**.

If you configure an access point provision list, only the access points in the provision list are provisioned when you enable AP provisioning. If you do not configure an access point provision list, all access points with a MIC or SSC certificate that join the controller are LSC provisioned.

10. Click **Apply** to commit your changes.

Local Significant Certificates (LSC)

General **AP Provisioning**

Enable AP Provisioning

Number of attempts to LSC (0 to 255)

AP Ethernet MAC Addresses

Add

MAC Address

Configure the Wireless LAN Controller through the CLI

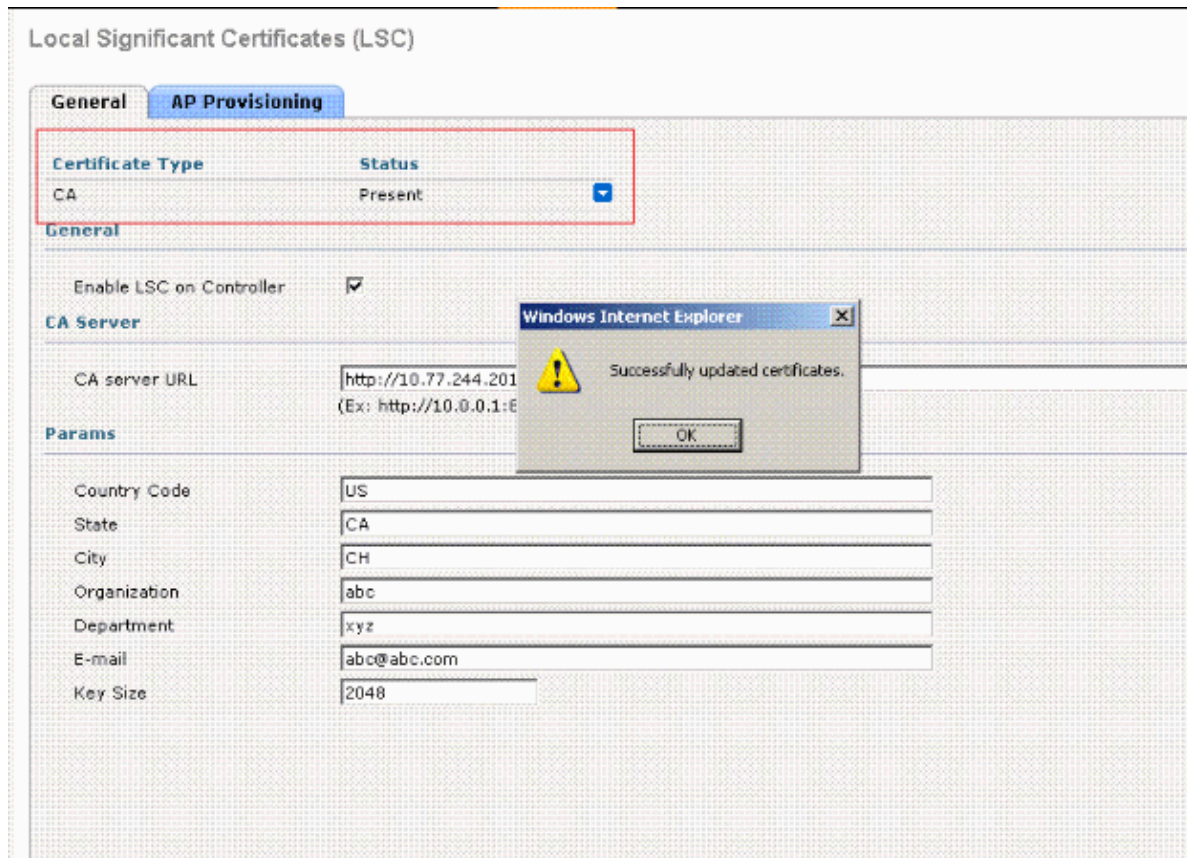
Refer to the **Using the CLI to Configure LSC** section of Cisco Wireless LAN Controller Configuration Guide, Release 5.2 for information on the procedure to enable the Locally Significant Certificate (LSC) feature from the CLI on the controller.

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Once the Wireless LAN Controller is configured and the CA server is in place, the Wireless LAN Controller uses the SCEP protocol in order to communicate with the CA server and acquire the LSC certificate. Here is a screenshot of the WLC once the certificate is installed.



When the LAP comes up, the LAP discovers the WLC with the Layer 2/ Layer 3 discovery mechanisms and sends a Join Requests to controller with the MIC certificate.

The Wireless LAN controller then sends the LSC certificate parameter request to the LAP.

With the SubjectName/CN sent from the WLC, the AP generates PKCS #10 CertReq and sends a LWAPP LSC Certificate Request to the WLC.

This request is in turn forwarded by the WLC to the CA server. The CA server sends the LAP LSC certificate to the controller. The controller then sends the LSC to the LAP.

This message appears on the AP CLI.

```
The name for the keys will be: Cisco_IOS_LSC_Keys
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]
LSC CA cert successfully imported
LSC device cert successfully imported
```

Finally, LAP sends a join request with the LSC.

Issue the **debug capwap events enable** command in order to view this sequence of events.

Once the LAP registers with the WLC with the LSC, you can confirm this on the WLC GUI.

Search by AP MAC

AP Name	AP MAC	AP Up Time	Admin Status	Operational Status	AP Mode	Certificate Type	AP Sub Mode
AP1130	00:16:c7:a0:eb:3e	0 d, 00 h 01 m 20 s	Enable	REG	Local	LSC	None

You can also use these commands from the WLC CLI in order to verify this. Here is an example:

```
show certificate lsc summary
```

```
Information similar to the following appears:
```

```
LSC Enabled..... Yes
LSC CA-Server..... http://10.77.244.201:8080/caserver
```

```
LSC AP-Provisioning..... Yes
    Provision-List..... Not Configured
    LSC Revert Count in AP reboots..... 3
```

```
LSC Params:
```

```
Country..... 4
State..... ca
City..... ch
Orgn..... abc
Dept..... xyz
Email..... abc@abc.com
KeySize..... 2048
```

```
LSC Certs:
```

```
CA Cert..... Not Configured
RA Cert..... Not Configured
```

In order to view details about the access points that are provisioned with LSC, enter this command:

```
show certificate lsc ap-provision
```

```
Information similar to the following appears:
```

```
LSC AP-Provisioning..... Yes
Provision-List..... Present
```

```
Idx          Mac Address
---          -
1            00:18:74:c7:c0:90
```

Troubleshoot

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

Related Information

- [Cisco Wireless LAN Controller Configuration Guide, Release 5.2](#)
- [Certificate Signing Request \(CSR\) Generation for a Third-Party Certificate on a WLAN Controller \(WLC\)](#)
- [Certificate Signing Request Generation for a Third-party Certificate and Procedure for Uploading Chained Certificates to the WLC](#)
- [Wireless Support Page](#)
- [Technical Support & Documentation – Cisco Systems](#)

