Elektron Administrator's Guide

Version 1.0 for Mac OS X

Corriente Networks LLC
Berkeley, California
www.corriente.net

Copyright © 2004 Corriente Networks LLC. All Rights Reserved.

Corriente Networks LLC
1563 Solano Avenue #484
Berkeley, California 94707
United States of America

http://www.corriente.net

Technical Suport: support@corriente.net
Other Inquiries: info@corriente.net

Contents

Getting Started With Elektron **5**
- **What You Will Need** **5**
- **Installing Elektron** **6**
- **Initial Configuration** **6**
  - Serial Number 6
  - Access Point Password 7
  - Digital Certificate 8
- **Configuring Access Points** **10**
  - Airport Express and Airport Extreme 11
- **Configuring Wireless Clients** **13**

Wi-Fi Security **15**
- **Requirements** **15**
  - Authentication 15
  - User Authentication 16
  - Server Authentication 16
  - Privacy 17
- **Wired Equivalent Privacy** **17**
  - WPA Personal 19
  - The Future of WPA 21
  - Deploy WPA-Enterprise 22
  - Protect Against Rogue Access Points 22
  - Do Not Rely On Physical Boundaries 23
  - Hide Your SSID 23
  - Protect Internal Services 23

Digital Certificates **25**
- **Your Server's Digital Identity** **25**
  - Distinguished Names 26
  - Contents of a Digital Certificate 27
  - Creating Trust 30
  - Certificate Chains 30
  - Certificate Signatures 31
  - Additional Certificate Validation 32
- **Public Key Infrastructure** **33**

Configuring Elektron **35**
- **Accounts** **35**
  - Mac OS X Accounts 35
  - Elektron Accounts 36
  - Access Point Password 38
  - Restrict Access Points to Local Network 38

Certificate Authority 39
Export Certificate Authority 39
Certificates 39
Active Certificates 39
Pending Certificates 41
Server Logs 41
Access Log 41
Error Log 42
Settings 42
Advanced 42
Enable IP Version 6 Services 43
Bind the Server to a Specific IP Address 43
Primary Server Port 43
Secondary Server Port 43
License 43
Serial Number 43

Configuring Clients 45
Windows XP 45
System Requirements 45
Installing the Elektron Certificate 45
Selecting Your Network 46
Mac OS X 53
System Requirements 53
On Demand Configuration 53
Full Configuration 56

Getting Started With Elektron 1

This chapter will walk you through the process of installing Elektron and performing its initial configuration.

What You Will Need

There are three main components in a secure wireless network: clients, access points, and the Elektron server that provides authentication services on the network. Each has their own requirements:

Elektron A PowerMac running Mac OS X or Mac OS X Server version 10.3 or later. This machine that hosts Elektron must be connected via the wired ethernet network. Elektron cannot provide services to the wireless network if is itself connected via the wireless network.

Wireless Clients For Windows clients, Windows XP with the latest service packs installed and a WPA-capable Wi-Fi card are required. For Mac OS X users, Mac OS X 10.3 or later and an AirPort or AirPort Extreme card is required. Elektron uses standard RADIUS/802.1X authentication, so other WPA Enterprise clients are likely to work as well.

Access Points Access points that will use Elektron services must support WPA Enterprise security. Many of the access points available today support WPA Enterprise, since the Wi-Fi Alliance has been requiring this support as part of their "Wi-Fi Certified"

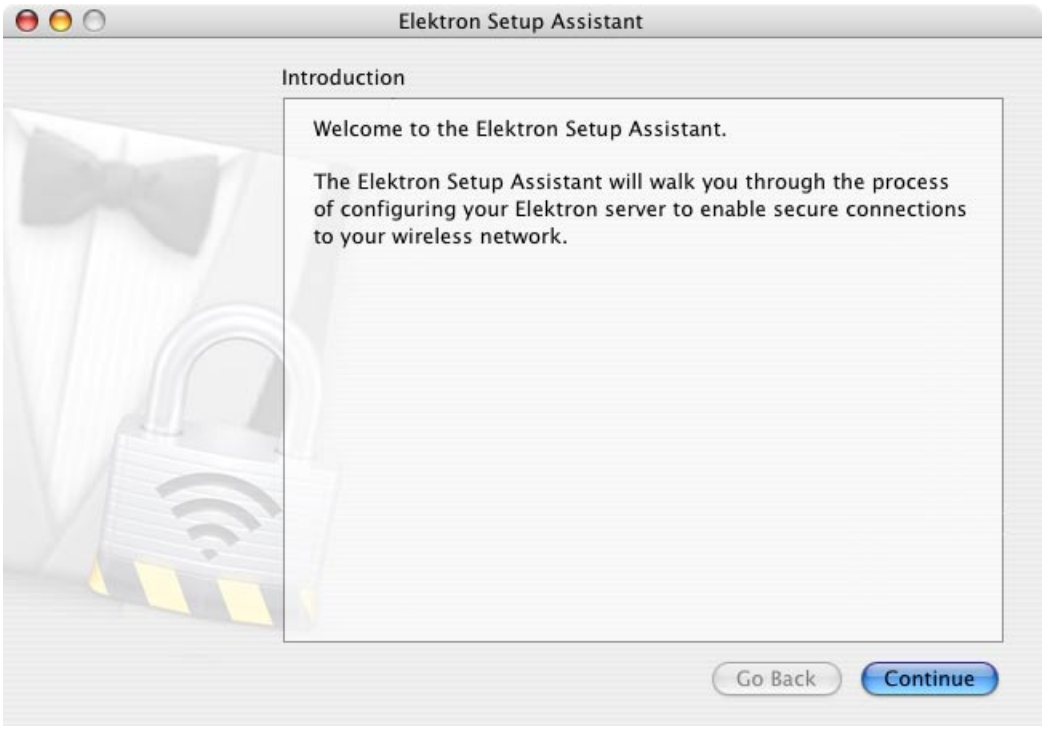
program. The Wi-Fi alliance maintains a list of Wi-Fi Certified access points at their web site, http://www.wi-fi.org. Popular recent access points from makers like Linksys, D-Link, Cisco, and Apple fulfill this requirement.

Installing Elektron

Begin by inserting the Elektron CD (for purchased hard copies of Elektron) or double-clicking the Elektron.dmg disk image (for downloaded copies of Elektron). Open the Elektron volume on your desktop, and double-click "Elektron.pkg". This will launch the installer application and walk you through the process of installing Elektron. This installer will work for both initial installations and upgrades.

Initial Configuration

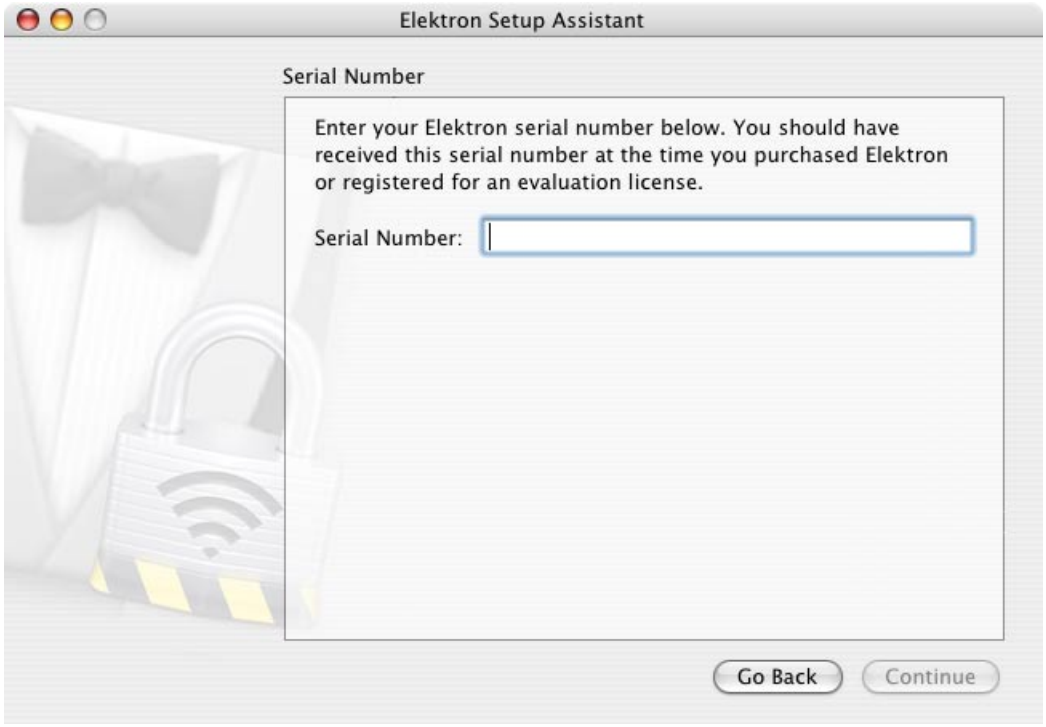
After the file installation completes, the installer automatically launches the Elektron Setup Assistant. This assistant provides a guided, step-by-step initial configuration of your Elektron server.



Serial Number

The first item the Elektron Setup Assistant asks for is your serial number. Enter the

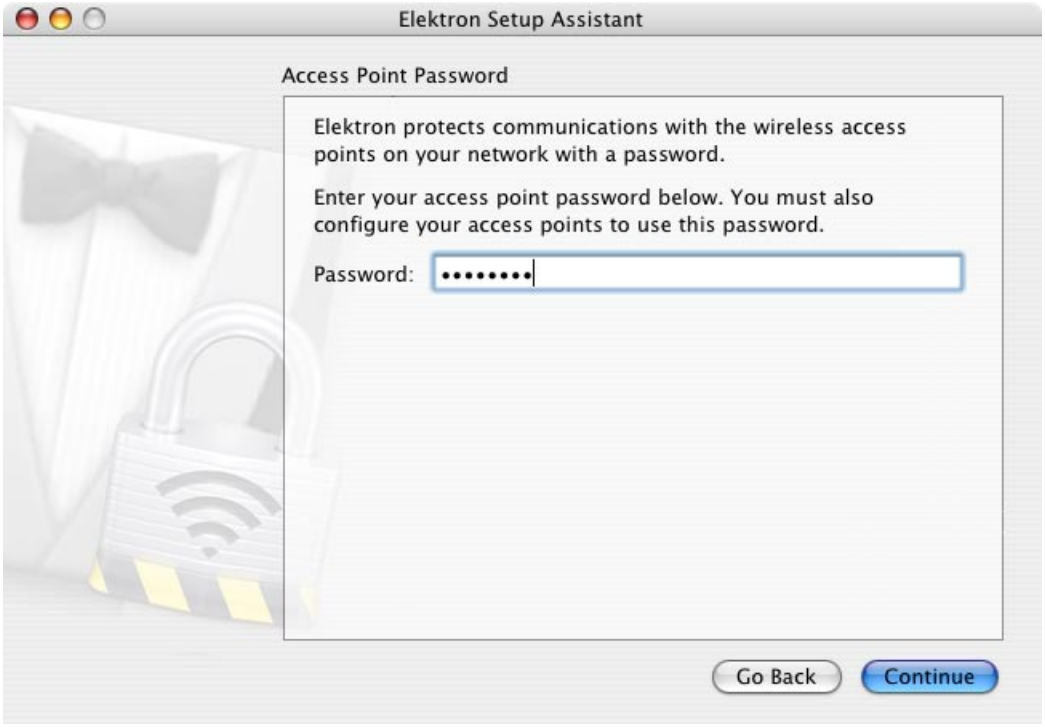
serial number you received at the time you purchased Elektron or registered for an evaluation license. For users who purchased the Elektron CD, your serial number can be found on the back of the CD case.



Configuration cannot continue until a valid serial number is entered. If you do not have a serial number, you can obtain one by purchasing a copy of Elektron or registering for an evaluation copy on our web site, http://www.corriente.net.

Access Point Password

Elektron secures communications with your network's access points by means of a shared secret, i.e., a password or passphrase. You will need to enter this password here in the Elektron Setup Assistant, as well as on each of the access points that will be used on your network. You will need to enter the password here exactly as it will be entered on your access points. Access point passwords are case-sensitive.

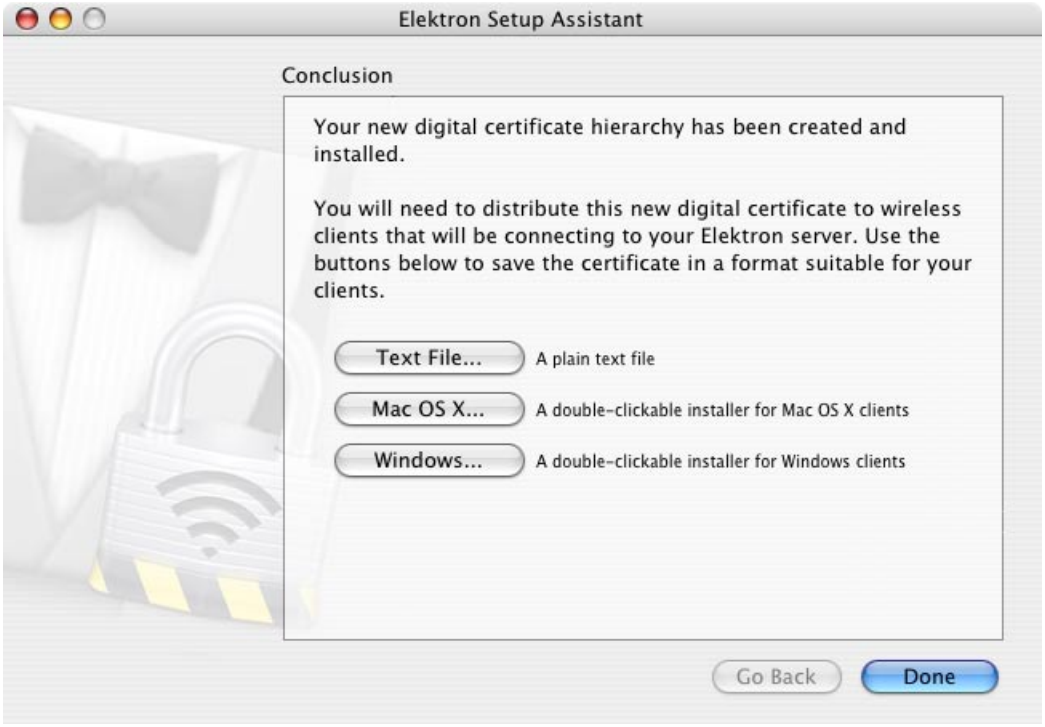


Digital Certificate

Every Elektron server needs a digital certificate which it uses to identify itself to wireless clients. During this portion of the configuration, you will be prompted for several pieces of information identifying your organization and server machine. Once this information is entered, you certificate will be created.

For the majority of users, accepting the "Create a new certificate hierarchy" option is the best combination of security and convenience. With this option, the Elektron Setup Assistant will prompt you for information about your organization and automatically generate a certificate hierarchy based on this information. Users with advanced PKI needs can select one of the other options as suits their needs, including integrating with an existing PKI or using an external CA such as Verisign. If you choose to go this route, be sure that the CA selected is capable of generating certificates compatible with WPA usage: some WPA clients (like the Microsoft Windows client) require specific certificate extension to be present in order to correctly authenticate the server.

After your certificate is created, configuration is complete. Your Elektron server is up and running and ready to accept incoming authentication requests.



On the final page of the Elektron Setup Assistant, you are provided with the option of saving your digital certificate in several different formats. These are needed in order to complete the configuration of clients that will be accessing your Elektron-protected Wi-Fi network. Clients use the Elektron digital certificate to confirm that they are communicating with a trusted server. You should export your certificate and distribute it to your wireless clients. If you choose to continue without saving the certificate at this point, you can always save it later from the "Identity" pane in the Elektron Settings application.

Some clients, such as the Mac OS X client, allow a user to connect to Elektron without having previously installed the Elektron digital certificate. In this case, a warning to the effect of "the server presented an unknown certificate, do you want to trust it anyway?" is presented to the user. Distributing the certificate to the user prior to the first login attempt will avoid this message, in addition to providing greater security.

To distribute the Elektron digital certificate to users, you can burn the installers to a CD that can be moved around to each client machine for its initial configuration. Another good option is to copy the installers to a keychain USB flash drive, and use the drive to install onto client machines.

Configuring Access Points

Each access point on your network must be configured to use your Elektron server

for user authentication and encryption key generation.

How to configure your access points will depend on what make and model of the units you are using. Consult your manufacturer's documentation on how to configure your specific access points.

The changes that need to be made to the access point configuration are:

Security Type Depending on your access point maker, this may be called "WPA Enterprise", "WPA-802.1X", "WPA-RADIUS", or something similar.

RADIUS Server Configure these settings to point to your Elektron server. You will need to enter your server's IP address and possibly the port on which the server is running. By default, Elektron uses port 1812.

Shared Secret This is the password use to secure communications between Elektron and the access point. Enter the shared secret with which you configured Elektron during the Elektron Setup Assistant process.

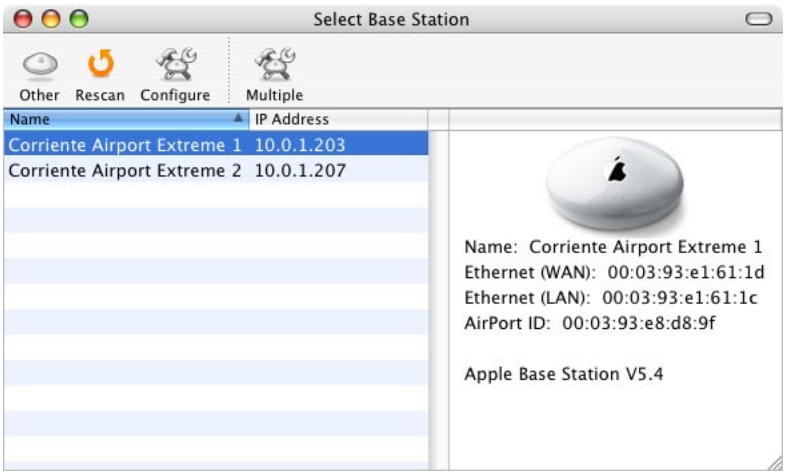
Some access points may allow more than one RADIUS server to be configured. This is to allow for fail-over in the event that the first RADIUS server is unavailable. You may choose to run multiple copies of Elektron running on different machines to provide this additional service, but you will need an additional license for each server deployed. For most small business networks, a single Elektron server will be sufficient.

AirPort Express and AirPort Extreme

Configuring either AirPort Express or AirPort Extreme base stations for WPA Enterprise security using Elektron is simple. Follow these steps to configure your base stations:

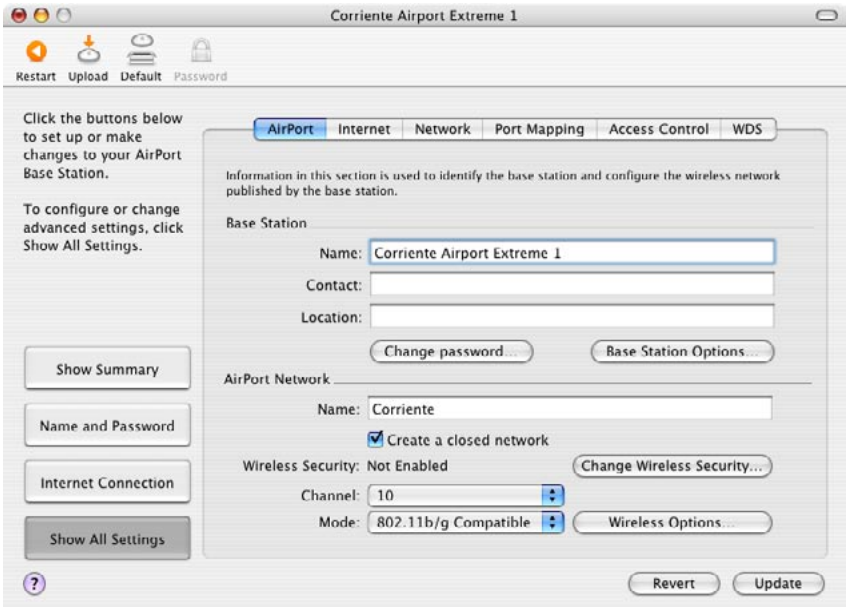
1. Launch the AirPort Admin Utility (located in /Applications/Utilities)

2. From the "Select Base Station" window, double-click the name of the base station to be configured



3. Enter the administrative password for the selected base station

4. On the left hand side of the resulting window, click the "Show All Settings" button



5. Click the "Change Wireless Security Options" button

6. Select "WPA Enterprise" as the Wireless Security option

7. You may be warned about your computer not being WPA capable. It is alright for the Elektron server computer to not be WPA capable: Elektron does not use the WPA protocol to communicate with your access points (it uses RADIUS, which in turn enables WPA for clients).

8. Enter the following values for Primary RADIUS Server (you may leave the Secondary RADIUS Server settings empty):

IP Address The IP address of the computer running the Elektron server

Port Enter the number "1812" (without the quotes, of course)

Shared Secret Enter the password you created when running the Elektron Setup Assistant, as described above in "Access Point Password"

Verify Secret Retype the password

Note that only AirPort Express and AirPort Extreme base stations are supported. Original graphite or snow AirPort base stations do not support WPA security.

Configuring Wireless Clients

Wireless clients that will be utilizing your secure network will require some configuration in order to join the network. This includes installation of the certificate authority's digital certificate on the client machines. For detailed information on how to configure both Windows and Mac OS X clients, see the chapter "Configuring Clients".

Wi-Fi Security

2

Wi-Fi networks have created productivity improvements in organizations, providing greater mobility to users by untethering them from the corporate network. This ease of access has also created new security headaches for network administrators: the same roaming access available to legitimate users is also available to potential attackers.

Requirements

The requirements for Wi-Fi security can be broken down into two primary components: authentication and privacy. Authentication ensures that only users who have been granted access to the Wi-Fi network are able to access the network, and privacy ensures that data transmitted on the Wi-Fi network is unavailable to unauthorized users. This chapter will discuss the issues involved in securing your Wi-Fi network and how Elektron helps solve the security problems associated with Wi-Fi networking.

Authentication

A critical element of Wi-Fi security is keeping unauthorized users off the network. Authentication is used to confirm the actual identity of a user or machine on a Wi-Fi network. Once a user's identity has been verified, the decision whether or not to allow access to the network can be made (in a process called authorization). Without performing strict identity checking on a network, attackers could access

protected resources on your network, either by pretending to be an authorized user and accessing the corporate network directly or by spoofing the corporate network and convincing legitimate users to login to the attacker's own false network.

In the context of Wi-Fi network security, there are two authentications being formed: the server that protects network access (e.g., Elektron) must authenticate the identity of the user attempting to access the network, and the user accessing the network must confirm the identity of the server.

User Authentication

The task of user authentication is performed by your Elektron server. In a typical Wi-Fi network login, a user will identify herself to the Elektron server by providing a username and password. Elektron will then verify that the username exists, and if so, that the password provided matches the password associated with the username in Elektron's database. If both conditions are met, the user is granted access to the network.

A risk in using password-based authentication is that during the login process the user must send to the server their username and password *before* the secure wireless channel has been established. This would leave the login prone to passive eavesdropping by an attacker. Secure Wi-Fi logins avoid this problem by establishing a encrypted channel that is used only for the login process prior to sending usernames and passwords. Once the user's identity has been established and access to the Wi-Fi network has been granted, the encrypted login channel is torn down and all wireless communications between the access point and the client are encrypted using a dynamic encryption key separate from that used during the login.

Standards bodies have defined a number of different methods of password-based user authentication. A number of these do not send the password in plaintext form, but rather as a cryptographic digest, in an attempt to mask the password from potential attackers. Some of these methods are also designed to provide mutual authentication (i.e., the server can authenticate the client and the client can authenticate the server). However, none of the methods provide protection against man-in-the-middle attacks, nor do they protect the username in anyway. In order to protect against these and other attacks, Elektron encrypts all password-based logins (with the exception of LEAP, which we recommend against using if your client software supports either PEAP or TTLS).

Server Authentication

While Elektron is responsible for verifying the identity of users attempting to login to your Wi-Fi network, users have the responsibility to verify the identity of the

Elektron server. This is an important and sometimes overlooked aspect of network security. It is arguably the more difficult of the two authentications performed for Wi-Fi network access, as it requires configuration of each client machine that will be accessing the network.

Unlike users, which typically identify themselves using a username and password, Elektron proves its identity using a digital certificate. Validating the server's digital certificate can happen automatically within the user's wireless networking client software, provided the client software has been pre-configured to recognize the certificate authority that issued the server's certificate (client configuration of the Windows 2000 and XP clients and the Mac OS X client is covered in the chapter "Configuring Client Software", while digital certificates are discussed in the chapter "Digital Certificates").

In order to verify the server's identity, users must perform digital certificate chain validation (as described in the chapter "Digital Certificates"). If the digital certificate validation fails, then the Elektron server's identity could not be verified and the Wi-Fi network access attempt should be terminated by the user. Such a failure can be indicative of a attacker attempting to lure a legitimate user into logging into fake network, thus fooling the user into giving up their username and password. Once armed with the user's credentials, the attacker can then use them to login to legitimate corporate network.

Privacy

In addition to authentication, a secure wireless network requires privacy. A traditional wired network can rely on its physical security to remain protected. So long as an attacker cannot physically connect to the wired network, the attacker cannot access data flowing across the network. A wireless network does not respect an organization's physical boundaries, so an attacker need only be in proximity to a wireless network to compromise it.

While authentication can prevent an attacker from actively joining a wireless network, encryption can prevent passive eavesdropping of user data. An attacker with a packet sniffer sees only scrambled bits. This keeps sensitive business information such as email and files private as users access corporate servers via the wireless network.

Wired Equivalent Privacy

The first attempt at keeping wireless networks private was a protocol known was Wired Equivalent Privacy (WEP). It was designed to be easy to deploy, and as its name suggests, to provide a level of security equal to that of a wired network. For a time it was the only means of security available in wireless hardware.

WEP Security Issues

WEP clients and access points encrypt their communications using a key shared amongst all users. This makes for easy configuration: simply enter the key into each piece of wireless hardware that will be on the network. However, while having shared keys makes system administration easier, it is also WEP's Achilles' heel, introducing two significant security holes into the protocol.

Lost Hardware

The first security hole associated with the use of shared keys is the potential abuse of lost or stolen hardware. Laptops, PDAs, and other Wi-Fi devices must have the network WEP key stored in order to participate in the network. If the device is lost, that key could fall into the hands of an attacker. If an attacker has possession of the network WEP key, then the attacker can participate on the network as well as decrypt the data encrypted by any other device on the network.

If a Wi-Fi device is lost or stolen, the network WEP key must be changed in order to maintain the security of the network. Because the key is shared by every device on the network, this mean re-configuring every device on the network.

Flawed Cryptography

The WEP protocol contains a serious flaw in its use of cryptography. WEP uses the RC4 algorithm to encrypt data packets. The RC4 algorithm is a well-known and widely used algorithm, and is safely used in many non-WEP applications. It is a stream cipher that supports variable-length keys, including the 40 bit and 128 bit keys used by WEP.

Researchers have discovered flaws in how WEP uses the RC4 algorithm. An attacker can passively eavesdrop on network traffic, and in a relatively short period of time recover the network WEP key. The attacker, armed with this key, can become a full-fledged user of the network.

Dynamic WEP Keys

The flaws in WEP and the lack of a viable alternative led some access point makers to come up with an interim solution: dynamic WEP keys. With dynamic WEP keys, each network user gets their own WEP key, which in turn is changed frequently. This solves the lost hardware problem, since no WEP key is stored. The flawed cryptography problem is mitigated by the frequently changing keys. The attacks on WEP's cryptography rely on a large number of packets being encrypted using the same key. Frequent key changes limit the number of such packets.

The method used to login to the wireless network and generate dynamic keys is defined in IEEE standard 802.1X. This is the same method used by WEP's successor, Wi-Fi Protected Access. Although Elektron was intended to be used with WPA networks, it can also provide services to WEP/802.1X networks as well.

Wi-Fi Protected Access

As wireless networking gained in popularity, its security shortcomings became increasingly apparent. In response, the IEEE began work on a new standard designed to address these shortcomings. This new standard, dubbed 802.11i, began to work its way through the lengthy IEEE review and approval process. In the meantime, the Wi-Fi Alliance, an industry trade group, created an interim standard called Wi-Fi Protected Access (WPA).

The primary new feature of WPA is the appearance of the Temporal Key Integrity Protocol (TKIP) in place of basic RC4 encryption. TKIP continues to use RC4, but in a more secure way than WEP. The initialization vector in TKIP is increased from 24 bits to 48 bits, per-packet key mixing is added to increase the difficulty in divining a network key, as well as a Message Integrity Check (MIC) to confirm that a packet has not been tampered with.

WPA is available in most Wi-Fi hardware produced today. In order to be considered "Wi-Fi Certified" by the Wi-Fi Alliance, access points and client hardware must support WPA.

WPA comes in two flavors: WPA Personal and WPA Enterprise. As the names suggest, the former was intended for small office/home office use, while latter was targeted toward large organizations. Elektron enables the use of WPA Enterprise for organizations of any size.

WPA Personal

In an effort to simplify WPA deployment for small networks, the Wi-Fi Alliance defined the WPA Personal mode. This mode is also known as WPA-PSK (Pre-Shared Key). Like WEP, it uses a single master key for all participants in the network. Thus, like WEP, it suffers from the security issues associated with using a single key for all users.

Like WEP, WPA Personal has its shortcomings, but is far better than no security at all. With WPA Personal enabled on their network, administrators can limit network access to users that have been provided the WPA key, while also encrypting data transmitted on the network.

WPA Enterprise

The WPA Enterprise mode is the most secure method available for locking down Wi-Fi networks, enhancing both authentication and privacy. WPA Enterprise provides for a separate username and password for each network user. It also generates dynamic keys that are unique to each user and that are changed frequently.

WPA Enterprise utilizes the 802.1X/EAP protocol to authenticate users, and thus requires a server to provide this authentication. This is the role filled by Elektron.

There are a number of advantages to using Elektron to provide WPA Enterprise services to your network over using WPA Personal:

User Management Each network user gets her own login, meaning that when if a user leaves your organization and will no longer have access to the network, only that user's credentials are affected. Under WPA Personal, all systems must be reconfigured to use a new master key.

Authentication Elektron can maintain its own database of users, or use operating system services to check logins. On Windows, this means that the Active Directory or SAM database can be used, and on Mac OS X Open Directory can be used. This means that only one user database must be maintained, so changes such as adding or removing users need only happen once.

Auditing Because each user has her own username, it is easy to keep track of who is logging into your network, and when.

Encryption Dynamic encryption keys are generated for each user at each login, and then changed frequently. This means that attackers should be unable to determine any user keys. What's more, because each user's key is unique, no user will be able to decrypt another user's network transmissions.

A WPA Enterprise Walk-Through

In order to connect to a WPA Enterprise protected network, a wireless client must go through several steps:

Step 1 First, upon initial connection to the wireless access point, the wireless cli-

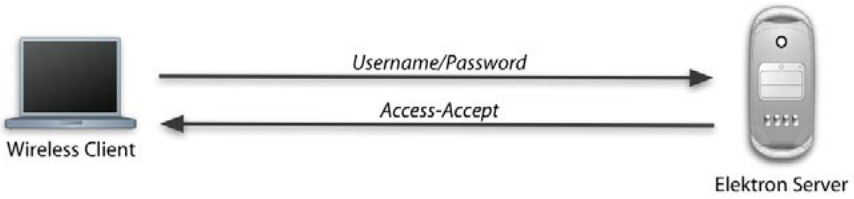
ent will be informed that WPA Enterprise authentication is required. At this point, the client is not allowed to forward any non-authentication related data packets to the wireless network.

Step 2 The wireless client initiates a WPA Enterprise login. Once the login process begins, the access point begins forwarding data received from the client to the Elektron server, and vice versa. It is Elektron's responsibility to manage the client login; the access point merely forwards packets back and forth between the client and server. While in this state, the access point will continue to disallow any non-login related data packets from the client.

Step 3 The client creates a TLS connection to the Elektron server. This will establish the server's identity and protect further communications from eavesdropping.

Step 4 While establishing the TLS connection, Elektron sends to the client its digital certificate. The client must verify the certificate's authenticity in order to continue with the connection (see the chapter "Digital Certificates" for more information). If the server's certificate cannot be authenticated, the client should terminate the login. Doing so can help prevent the client from inadvertently sending their login information to an attacker.

Step 5 After the TLS connection is established and the server's identity is confirmed, the client sends her username and password. Elektron validates the username and password, sending either an "access-accept" or "access-reject" message to the client.



Step 6 If the result is "access-accept", Elektron sends to the access point the dynamic keys to be used for encrypting the wireless session. The client computes these keys itself, and the secure wireless session begins.

The wireless login process is transparent to the user, with all of the details handled by Elektron and the client software.

The Future of WPA

As described above, WPA is an interim specification designed to bridge the gap between WEP and the adoption of IEEE 802.11i. The intent was to get stronger security into the hands of users as quickly as possible. WPA provides a subset of 802.11i that can be implemented by hardware manufacturers and software developers without having to require replacement of existing equipment. In fact, most Wi-Fi equipment sold today is either WPA capable out of the box or is firmware-upgradeable to support WPA. The Wi-Fi Alliance requires that all "Wi-Fi Certified" equipment support WPA.

The future of WPA is the adoption of the full 802.11i specification rather than the subset supported now. Some of the new features of 802.11i are:

AES Encryption The option to use the federal Advanced Encryption Standard as the algorithm used to encrypt data packets in place of the Temporal Key Integrity Protocol (TKIP). Some Wi-Fi equipment makers are shipping AES with their products today.

Secure Fast Handoff This allows roaming between access points without requiring clients to fully re-authenticate to every access point. Re-authentication can slow roaming, disrupting real-time networking applications like multimedia or VoIP.

Secure IBSS Independent Basic Service Set (IBSS) wireless topologies, sometimes called ad-hoc networks, receive new security features in 802.11i.

Best Practices

There are a number of actions that a network administrator can take to ensure that their wireless network is as secure as possible.

Deploy WPA Enterprise

If you are reading this manual, chances are that you've already made the decision to deploy WPA Enterprise security on your wireless network. Elektron is a key component of a WPA Enterprise network, providing the necessary RADIUS/802.1X authentication services to the network's access points.

Protect Against Rogue Access Points

A rogue access point is any access point not officially installed by the network administrator as part of the secure wireless network. Typically, there are installed by legitimate users who have decided not to wait for the network administrator to install Wi-Fi or have decided on their own to extend the Wi-Fi network's range. While their intentions may be good, these users can inadvertently open up gaping security holes in the corporate network.

In more extreme cases, a rogue access point could be installed by an attacker as means to compromise a network. By installing a rogue access point, an attacker need only physically break into a network once (for the initial access point installation). Any future network intrusions can be made remotely via the rogue access point.

Protecting against rogue access points can be difficult. Network administrators can use the same tools that wardrivers use to find open access points, such as NetStumbler, to home-in on rogue access points. There are also dedicated systems specifically designed to track down rogue access points on a network. And because the rogue access point must at some point connect to the wired network, an administrator can also monitor ethernet switches and hubs to ensure that no unauthorized devices are connected.

Do Not Rely On Physical Boundaries

There is no reliable way to ensure that the RF signals on your wireless network stop at the physical boundaries of your company. Attackers using devices such as range-extending antennas may still be able to pick up your network's signals. If you deploy a wireless network, you must assume that an attacker has access to it. For this reason, you must use all available means to lock down your network.

Hide Your SSID

Service Set Identifiers (SSIDs) are used by access points to advertise their availability to potential clients. Access points broadcast their SSID to client applications, which can present the user with a list of all nearby networks. Many access points allow the network administrator to remove the access point's SSID, thus preventing the access point from broadcasting its availability.

Removing the SSID is far from foolproof security, but it does add at least a small extra layer of protection. Users must know the network SSID before logging into the network, which conceivably could keep intruders out.

Protect Internal Services

It's good practice for network administrators to be paranoid. All network servers should be kept as secure as possible, with the assumption that attackers have access to the network. This includes maintaining a strong password policy and keeping Access Control Lists (ACLs) up to date in order to limit network resources to legitimate users.

Digital Certificates

3

Your digital certificate is a critical element of your Elektron configuration. Every Elektron installation requires a digital certificate so that the server can identify itself to wireless clients. This chapter introduces the concepts of digital certificates, including how they are constructed and how they protect your wireless network.

Your Server's Digital Identity

The primary purpose of a digital certificate is to cryptographically bind a public key to a name. In layman's terms, a digital certificate is a secure way for one computer to tell another computer "here's who I am, and here's my key." Certificates allow a neutral third party, called a certificate authority (CA), to vouch for the identity of a user or computer by using their own digital certificate to sign the user or computer's certificate.

The format and usage of digital certificates is defined by ITU-T Recommendation X.509 and further refined in IETF RFC 2459. If you are interested in the technical details of digital certificates, consult these references. The following description should suffice to get your Elektron server up and running securely.

Distinguished Names

Because the purpose of a digital certificate is to bind a public key to a name, there must be a way to encode names so that they can uniquely identify any person or computer on the planet. To solve this problem, the "distinguished name" was created by the developers of the X.500 series of technology standards. Distinguished names create a hierarchical tree of named objects using one or more of the following fields:

Country This is the two-character ISO country code for the country in which the person or computer identified by the digital certificate is located, for example "US" for the United States or "CA" for Canada.

State or Province The non-abbreviated name of the state or province where the certificate holder is located.

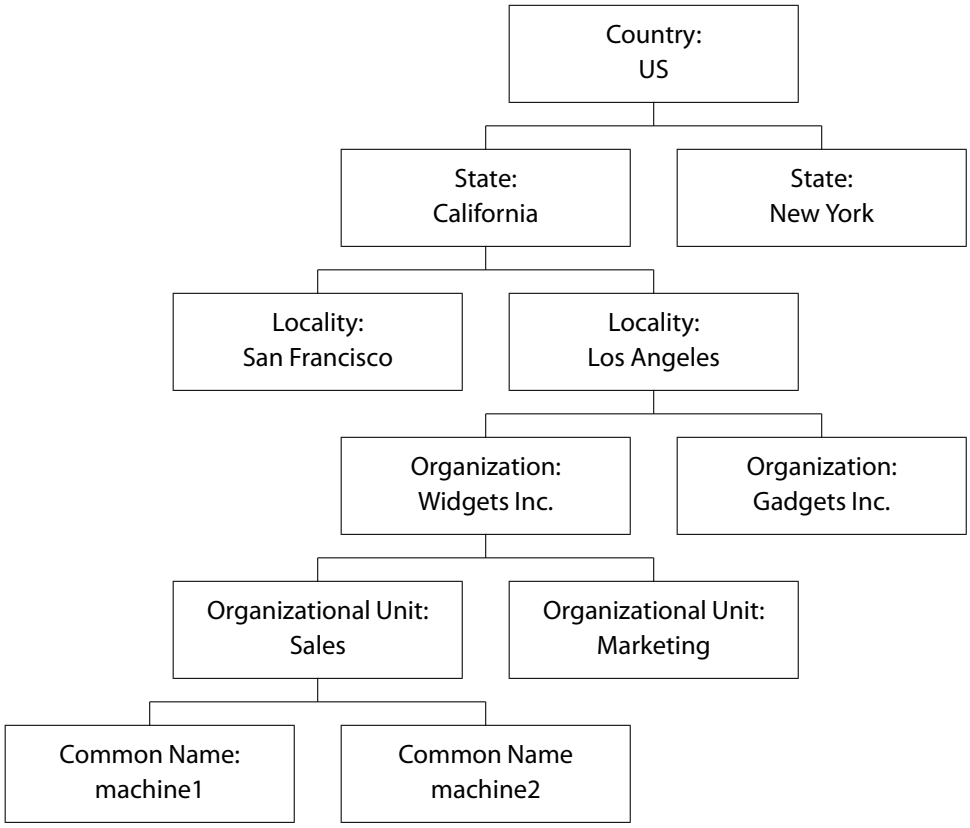
Locality The locality is the third and final of the geographic identifiers. As the name suggests, it is the city in which the certificate holder is located.

Organization If the certificate holder is part of a business, this is the business' name. For educational users, the name of the educational institution.

Organizational Unit This field is intended to designate the certificate holder's department within the organization. In practice, many certificate authorities use this as a free-form field in which to place informational data.

Common Name This is the final field which uniquely identifies the certificate holder within the organization. For a computer application, such as your Elektron server, this field will contain the DNS name of the computer, such as "machine.example.com". If the certificate identifies a person, this will contain the person's name, such as "Alice Smith".

This naming scheme creates a hierarchical structure wherein each subsequent element of the name zeros-in on the specific object identified by the name, as in the figure below.



A distinguished name hierarchy.

The concept of distinguished names should be familiar to LDAP users, since LDAP uses them to identify objects in the LDAP directory. Both LDAP and X.509 digital certificates like those used in Elektron trace their lineage back to the X.500 standards.

Distinguished names in their natural form are binary data encoded using Abstract Syntax Notation (ASN.1). For human consumption, distinguished names can be formatted as strings. In this case, each field is listed as an attribute-value pair, with the attribute name abbreviated to one or two characters, for example, "C=US, ST=California, L=Berkeley, O=Corriente Networks LLC, CN=example.corriente.net".

Contents of a Digital Certificate

At its simplest, a digital certificate is nothing more than a computer data file, much like a word processing or spreadsheet file. Typically, digital certificates ranges from a few hundred to a few thousand bytes in length. There are a number of different ways a digital certificate can be stored as a file on disk, such a in binary form (using Distinguished Encoding Rules, or DER), as a PKCS#12 file, or most commonly as a text file (sometimes called "PEM encoding"). Elektron uses text files to import and export certificates, in order to ensure the widest compatibility with

other digital certificate applications.

Inside each digital certificate are a number of different data fields, some of which are required and others which are optional. The contents of the certificate vary based on the identity of the certificate holder, the certificate authority that issued the certificate, as well as the version of the certificate. Digital certificates are available in two different versions: version 1 and version 3 (there was a version 2 defined, but it never made it into widespread usage). Elektron supports both digital certificate versions, although most Elektron installations will use only version 3 as that is the version required by most wireless clients. Here are the data fields present in a digital certificate:

Serial Number Every digital certificate includes a serial number to uniquely identify it. When used in combination with the issuer name and an outside source such as a certificate revocation list (CRL) or and online certificate status protocol (OCSP) responder, the serial number can help determine the certificate's current status. You should consult your client software documentation for information on configuring certificate status checking. Most small businesses will not require certificate status checking.

Issuer Name Certificates are digitally signed by a certificate authority. The issuer name field contains the distinguished name of the CA, allowing applications to recreate certificate chains in order to validate a given certificate. For a discussion of validating certificate chains, see below.

Validity Period Digital certificates have a time window during which they are valid. The validity period includes two dates: a "not valid before" date and a "not valid after" date. If a digital certificate is presented for validation outside these two dates, it should be rejected.

Subject Name The subject name contains a distinguished name that identifies the holder of the digital certificate. The format of distinguished names is described above.

Extensions These appear only in version 3 certificates. Extensions allow the certificate creator to insert data into the certificate that does not fit into the other fields. There are a wide variety of

extensions defined for use, including extensions describing what cryptographic purposes a certificate may be used for, whether a certificate may be used as a certificate authority, and alternative names for the certificate's subject. **You should note that some wireless clients, most notably the WPA client included with Microsoft Windows XP, require specific extensions to be present in the server's digital certificate.** In the case of the Windows XP clients, an Extended Key Usage extension designated "server authentication" must be present or Windows will reject the certificate. Elektron will correctly create certificates for use with Windows XP clients, but if you choose to generate your own certificates using another application or use a third-party Certificate Authority, you will need to ensure that the certificate includes the necessary extensions.

Public Key

Traditional cryptographic systems have used what is called "symmetric cryptography", in which a single key (such as a password) is used to encrypt data, and the same key is used to decrypt the data. Public key cryptography introduces the concept of "asymmetric cryptography", where a pair of keys is used: one to encrypt, another to decrypt. Any data encrypted with one key may only be decrypted with its paired key. No other key can be used to decrypt the data, including the key that was used to encrypt the data. Of the two keys in the key pair, one is known as the public key, which is distributed to other users. The other key is known as the private key, and is maintained securely by the key pair's owner.

Public key cryptography enables a number of solutions to problems that have plagued secure communications for centuries. One such problem is key distribution: in order to communicate securely with another person, you would first need to somehow securely transmit the key used to encrypt the data you are sending. If you are communicating with a number of different people, this can become unwieldy. Public key cryptography solves this problem by allowing you to freely distribute your public key with no need to keep it secret, since only you hold the private key, and any data encrypted using your public key can only be decrypted using your private key.

Every digital certificate contains the certificate holder's pub-

lic key, which can be used to verify signatures generated by the certificate holder, as described below.

Signature

Another feature of public key cryptography is the ability to generate digital signatures. A digital signature performs much like a traditional signature, in that it identifies the sender of a piece of data, but with the added ability to prove that the signed piece of data has not been altered since it was signed. Every certificate contains a digital certificate generated by the certificate authority that created the certificate. This allows anybody who receives the digital certificate to verify that it is the true and correct certificate as generated by the certificate authority.

It is the digital signature on a certificate that gives that certificate its trustworthiness. If a user trusts a given certificate authority, and the user receives a certificate signed by that certificate authority, the user can trust the certificate.

Creating Trust

A digital certificate by itself is of limited usefulness in terms of establishing the identity of the certificate's owner. For instance, when a wireless client connects to your Elektron server, Elektron will send its digital certificate to the client. It is not enough for the client to merely look at the name on the certificate, it must verify the signature on the certificate and trace it back to a certificate authority that is trusted by the client.

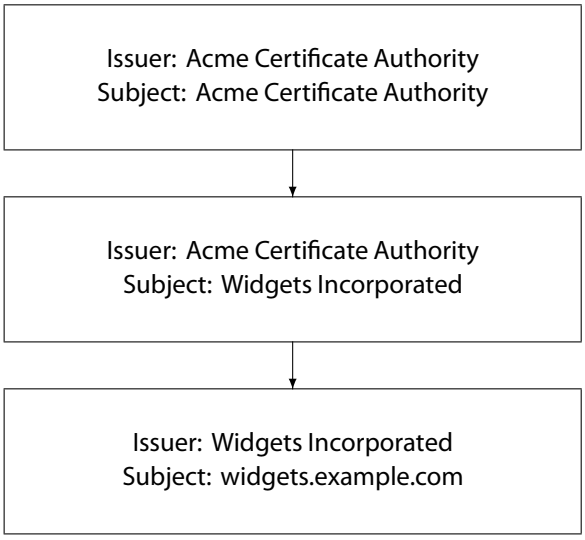
Certificate Chains

In order to verify the trustworthiness of a certificate, a client must build a certificate chain to trace it back to a trusted source. Many wireless clients, including those built in to Windows and Mac OS X, come pre-configured with a database of certificate authorities that will be trusted automatically. Any server sending a certificate signed directly by one of these pre-configured certificate authorities will be considered trustworthy. Additionally, any certificate that can be chained back to one of these certificate authorities will be trusted.

Given a server's certificate and a database of trusted certificate authorities, the client can construct the certificate chain by using the certificate's subject and issuer name fields. Starting with the server certificate's issuer name, the client searches its certificate database for a certificate with a matching subject name. If one is found, the public key from the issuer certificate is used to verify the signature on

the subject's certificate. If the signature verifies correctly, then the client continues to build the chain by looking for the issuer of the previous issuer's certificate, until the chain is complete.

At the end of each chain is a self-signed root certificate. This is a digital certificate where the issuer and subject names are the same, and the public key in the certificate is able to verify the signature on the certificate. Self-signed root certificates are held by certificate authorities, and are used to solely sign other certificates.



An example certificate chain.

In the example certificate chain shown above, the self-signed root certificate is held by the fictional Acme Certificate Authority. The second certificate in the chain was issued by the Acme Certificate Authority to Widgets Incorporated. In this example, the Widgets Incorporated certificate is acting as an intermediate certificate authority, which issued the final certificate in the chain, the widgets.example.com certificate.

A wireless client connecting to the widgets.example.com server would need to have either the Widgets Incorporated or the Acme Certificate Authority in its database of trusted certificate authorities. If either of these were present in the trusted database, then the widgets.example.com certificate would itself be trusted. In effect, the client is saying, "the widgets.example.com certificate is signed by the Widgets Incorporated certificate authority, and I trust Widgets Incorporated, therefore I can trust widgets.example.com".

Certificate Signatures

The digital signature on a certificate is the key to verifying the certificate's trustworthiness. When a certificate authority signs a certificate, the authority is signal-

ing that the certificate holder's identity has been verified and that the certificate holder can be trusted to conduct secure transactions using the certificate.

Because individual users are unlikely to have the time or inclination to accurately verify the identity of a certificate holder, users must rely on certificate authorities to perform that task. Users can then keep a limited number of certificate authorities that they trust to make identity decisions on their behalf, and when receiving a certificate signed by one of these authorities, the certificate can be trusted.

There are a wide variety of certificate authorities for users to choose from. Commercial authorities, such as Verisign and GeoTrust are commonly used by web site operators to secure e-commerce sites. For proprietary networks, such as your small business wireless network, a good solution is to act as your own certificate authority. This can be both less expensive (commercial certificate authorities charge hundred of dollars for a certificate), and less hassle (commercial certificate authorities typically require that you renew your certificate every year).

If you use the Elektron Setup Assistant to configure your Elektron server, a variety of options are available for choosing a certificate authority. The default (and recommended) option is to create a new certificate chain while acting as your own certificate authority. After running the Elektron Setup Assistant, you will have a certificate that can be distributed to wireless clients for inclusion in their databases of trusted certificate authorities.

Additional Certificate Validation

While validating the signatures on a digital certificate chain is a key part of validating the authenticity and reliability of a certificate, it is not the only step that must be performed. Any application accepting digital certificates must also perform checks on these features:

Validity Period The application must determine that the certificate falls within the dates specified as the certificates validity period.

Name Checking The subject name in the certificate must match the name expected by the client application. This can prevent an otherwise valid certificate chain from being used in an invalid context. For instance, if you were to purchase a book from Amazon.com's secure web checkout, you would want to ensure that the name on the digital certificate used to secure the site is "www.amazon.com".

Extensions

The application must check extensions present in the certificate to ensure that the certificate is being used in a manner consistent with what the certificate authority has authorized. The following are the most common checks performed on certificate extensions:

- The certificate is allowed to perform the basic operation it is being called on to perform, such as validating a digital signature or exchanging cryptographic keys (key usage checking).
- The application using the certificate is appropriate for the certificate. As mentioned above, Windows XP wireless clients require that the correct extension be present here in order to verify the certificate (extended key usage checking).
- Any intermediate certificate authorities in the certificate chain must be allowed to act as certificate authorities (basic constraints checking).

Revocation Status

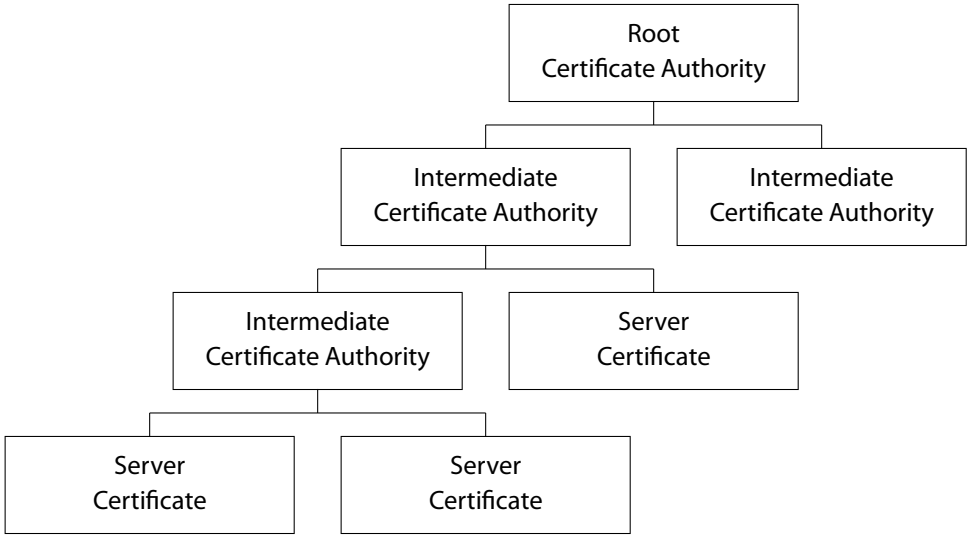
It is possible for a certificate to be revoked (that is, cancelled for usage) by a certificate authority prior to the end of its normal validity period. This can happen if the certificate holder's private key is compromised, the certificate holder's identity changed (for instance, their certificate identifies them as an employee of a certain company, and they leave the employ of that company), or under other circumstances. Since a certificate by itself only specifies a certificate's status at the time a certificate is issued, additional status checking at the time the certificate is actually presented is sometimes used. This usually comes in the form of a certificate revocation list (CRL). However, due to the complexity of keeping certificate status lists up to date, many organizations do not perform this checking.

Once these checks have been successfully performed, the client can accept the server's certificate and the wireless login process can proceed.

Public Key Infrastructure

Public Key Infrastructure (PKI) is the name given to the organizational deployment of digital certificates. At its simplest, a PKI may consist of only a single certificate chain, such as one generated by the Elektron Setup Assistant for your small business. As its most complex, a PKI may be a multi-tiered hierarchy consisting of

millions of certificates, such as the PKI maintained by the United States federal government for its employees.



A hierarchical PKI.

If you choose to purchase a digital certificate from an external certificate authority for use with Elektron, you will be participating in that certificates authority's PKI.

If you are deploying Elektron as part of a larger PKI, you can use the Elektron Set-up Assistant or the Elektron Settings application to generate a certificate request that can be submitted to your certificate authority for fulfillment.

Configuring Elektron

4

This chapter shows you how to use the Elektron Settings application to configure your Elektron server to suit your needs. The Elektron Settings application is installed into the system-wide Applications folder.

Accounts

One of Elektron's primary functions is to authenticate users by comparing their username and password against a database of login information in order to determine if a given user should be allowed to access the wireless network. The Accounts pane lets you control how Elektron authenticates users.

Elektron can use one of two methods to authenticate user logins: using operating system accounts, or using its own internally maintained database of user accounts.

Mac OS X Accounts

When authenticating wireless users with Mac OS X system accounts, users will use the same username and password that they use to login to the computer or to access Mac OS X system services like file sharing. The advantage of using this method is that usernames and passwords are kept in a single place, making the task of adding, editing, or removing users easier. The disadvantage to this method is that creating system accounts grants these users at least some access to the rest of the system, even if the intention is only to allow these users access to the wireless network. That is, there is no way to specify "this account is for wireless network access

only" when creating a Mac OS X system account.

Elektron Accounts

The alternative to using operating system accounts for authentication is to use Elektron to maintain user accounts separately. This allows you to grant access to your wireless network without granting access to the system hosting Elektron.

Elektron account configuration is available only when "Authenticate Wireless User Using Elektron Accounts" option is selected. To create a new Elektron user account, click the "+" button located below the list in the Accounts pane. To delete an Elektron account, select it from the list of accounts and click the "-" button.

The following options are available when configuring an Elektron user account:

Login Name This is the username that will be used to login to the wireless network. This can be a simple, unadorned username such as "alice", or may have a domain appended, such as "alice@corriente.net". Similarly, a Windows-style domain can be prepended, such as "CORRIENTE\alice", but Elektron stores domain names in "user@domain" format, so any usernames entered in the Windows format will be converted.

Full Name This is the user's real name, such as "Alice Smith". It is used for logging purposes, and is optional.

Password This is the password that will be required of the user when logging into the wireless network. You should create a password that is difficult to guess, and include in it mixed-case letters, numbers, and punctuation characters. Avoid words that appear in the dictionary. The tab and carriage return characters are not allowed in passwords. Spaces, however, are allowed, so you can create multi-word passphrases.

Password Storage With the "Store password in reversible format" option selected, the account password will be stored on disk in an easily decoded format. Leaving this option disabled will make the server more secure by only storing passwords in a hashed format, but will prevent some protocols that require the server to maintain a database of plain text passwords to authenticate.In this release of the server, the only protocols that requires plain text passwords are CHAP and EAP-MD5-

Challenge. For users with non-reversible passwords accessing the server via TTLS, an inner authentication method other than CHAP must be selected (PAP is the most common). For PEAP, an inner authentication method other than EAP-MD5-Challenge must be selected (EAP-MS-CHAP-V2 and EAP-GTC are most common).

Both the Windows XP and Mac OS X clients by default will use protocols that do not require reversible passwords to be enabled.

You may also configure search domains using the Domains button. This is a comma-separated list of domains that will be used to complete usernames that are submitted to the Elektron server for authentication unadorned.

For example, if an Elektron account were configured with the following username:

alice@corriente.net

And if the search domains field were configured as:

acme.com,corriente.net,domain.org

A user attempting to log in with the username:

alice

Would cause the Elektron server to first look for an account with the username alice, if that is not found it would look for an account with the username alice@acme.com, if that is not found, it would try alice@corriente.net. Upon finding an account with this username, it would continue by verifying the password submitted.

Search domains also allow you to store user accounts using unadorned names and allow users to log in using domain-adorned names. For instance, if Elektron is configured with the account for the username:

alice

And if the search domains field were configured as:

acme.com,corriente.net,domain.org

A user attempting to log in with the username:

alice@corriente.net

Elektron will use the "alice" account to verify the user's password.

You may leave this field blank, which will require that users login with the exact username assigned to their account.

Elektron also supports logins made using Windows-style domains, so the above examples also apply to the username CORRIENTE\alice as well as alice@corriente.net.

Access Points

Elektron needs to be able to communicate with the wireless access points on your network in order to authenticate users on behalf of the access points. The Access Points pane allows you to configure the options available for determining how Elektron talks to your access points.

Note that Elektron must be installed on a computer that is connected to your access points via your wired ethernet network. Elektron cannot communicate with access points using your wireless network.

Access Point Password

This is the password used by the access point and Elektron to authenticate and encrypt communications between the two. The password entered here must match exactly the password configured on the access point. The password is case-sensitive.

Consult the manufacturer's documentation for information on how to configure the shared secret on the access point.

Restrict Access Points to Local Network

You may choose to restrict which access points may use the server for authentication on the basis of the access point's IP address. If this option is enabled, only access points that are on the same subnet as the server (as determined by the server's IP address and subnet mask) will be able to connect to the server.

Identity

In order to provide trusted network security services to wireless clients, Elektron

must be able to cryptographically identify itself to clients. To prove its identity to clients, your Elektron server sends them its digital certificate during the client login procedure. The Identity panel allows you to select the digital certificate that your server will use.

While the Elektron Settings application allows you to manually configure digital certificate settings, we recommend that the Elektron Setup Assistant be used instead. The Elektron Setup Assistant will walk you through the step-by-step procedures needed to create and install a digital certificate.

For a detailed discussion of certificates, see the chapter "Digital Certificates".

Server Certificate

This popup allows you to select which digital certificate will be sent to wireless clients. To manage your server's digital certificates, use the Certificates panel.

Certificate Authority

Displays the common name of the certificate authority (CA) that issued the selected server certificate.

Export Certificate Authority

There are two digital certificates involved during the wireless login procedure: the server certificate, and the CA certificate.

Wireless clients verify the server's identity by validating the digital signature on the server's certificate. In order to validate this signature, the client must already have a copy of the certificate authority's digital certificate.

You can use the export buttons to transfer the CA certificate to clients.

Certificates

The Certificates panel allows you to manage the digital certificates that your Elektron server can use to securely identify itself to wireless clients. Using this panel you can view certificate information, request new certificates, fulfill existing certificate requests, and delete certificates and certificate requests.

We recommend that you use the Elektron Setup Assistant to manage your digital certificates.

Active Certificates

This tab shows the list of all available server certificates. To select the digital certificate to be used by Elektron, use the Identity panel. The following three buttons are available:

New Creates a new certificate request suitable for submission to a certificate authority. Clicking the New button brings up a sheet asking for the requested certificate's distinguished name. You should consult your chosen CA's guidelines for information on what to enter for each field. After you create the request, it will appear on the Pending tab. To export the certificate request for submission to your CA, select the request in the Pending tab and click the Edit button.

Edit Allows you to view the details of the selected certificate, and export the certificate as a text file. If no certificate is selected, the button is disabled.

Delete Deletes the selected certificate. If no certificate is selected, the button is disabled.

New Certificate Fields

When creating a new certificate request by clicking the "New" button, enter the following information:

Country Select the name of the country in which in the Elektron server is located. The Elektron Settings application will replace this name in the certificate request with the correct two character ISO country code.

State This field should contain the non-abbreviated state or province in which the server is located. If the server's location does not have a state or province, you may leave this field blank.

City Enter the city in which the Elektron server is located.

Organization This is the name of your organization. If your are creating this digital certificate on behalf of a company, enter the name of the company below. For an educational institution, enter the institution's name. If you are installing Elektron

as an individual, such as for a home office, enter your own name.

Department This is the group within your organization served by the Elektron server, such as "Sales and Marketing". If there is no specific department associated with the server, you may leave this field blank.

Name This is the fully-qualified domain name of your server, such as servername.corriente.net.

Public Key Type If your certificate authority requires a specific public key type or length, you may select here. A 1024 bit RSA public key should be acceptable to most certificate authorities.

Elektron Settings limits the characters that can be entered in these fields to those that are legal in the ASN.1 PrintableString type. The characters allowed are A-Z, a-z, 0-9, space, and '()+,-./:=?.

Your certificate authority (CA) may have specific requirements for certificate requests. Before creating and submitting your certificate request, consult the CA's documentation for these requirements.

Pending Certificates

This list shows all certificate request that are awaiting fulfillment by a certificate authority. The following two buttons are available:

Edit Allows you to view the details of the selected certificate request, and export the certificate request as a text file. If no certificate request is selected, the button is disabled. The Edit button also allows you to select a text file (i.e., a PEM file) that contains the fulfilled certificate.

Delete Deletes the selected certificate request. If no certificate request is selected, the button is disabled.

Server Logs

The server logs panel gives a view of your server's status and allows you to select

the level of logging provided. Server logs are loaded when Elektron Settings is launched, but are not automatically updated while it is running. To force an update of the log display, click the "Refresh" button.

Access Log

The Access Log tab displays recent login attempts. The information displayed in the Elektron Settings application Access Log tab includes whether the authentication was successful (green for success, red for failure), the date and time of the authentication, and the username presented.

The server access log file is located at:

/Library/Logs/Corriente/radiusd_access.log

The access log file includes some information not presented in the Elektron Settings user interface, including the type of authentication used and the RADIUS attributes that were sent by the access point requesting authentication.

Only login attempts that made it to the user authentication step are included in the Access Log. Any logins that were cancelled or otherwise failed before user authentication will be logged in the Error Log.

Error Log

The Error Log displays diagnostic messages about your Elektron server. If you are having trouble with your server, this is the first place to look. Information logged here includes user login failures (including the reason for the failure, such as a bad password or non-existent username), network problems, and digital certificate issues. The amount and detail of the information logged is determined by the option selected on the Settings tab.

The server error log file is located at:

/Library/Logs/Corriente/radiusd_error.log

Settings

You can select the amount of information logged in the Error Log by choosing the appropriate option from the Log Level popup. The available values are:

Minima	With this option selected, the only information logged is errors. No additional diagnostic information is included.
Normal	The Normal option includes all error messages, as well as

	warnings of issues that could affect the operation of the server.
Verbose	To include additional information to help troubleshoot connection problems, select Verbose.
Debug	This option includes the maximum amount of information, and includes detailed information about all aspects of the server operation. This option should only be enabled to debug connection problems, and disabled once the problems are resolved. **The Debug option may log sensitive information such as user passwords.** Use it with care.

Advanced

The Advanced panel gives you access to Elektron's networking options. Most users will leave these options untouched.

Enable IP Version 6 Services

With this option enabled, Elektron will attempt to bind to network interfaces using both IPv4 and IPv6 addresses. Since no wireless access points currently support IPv6, this probably isn't very useful to most users today.

Bind the Server to a Specific IP Address

If your network interface is configured with multiple IP address, you may choose to enter one here in order to limit the availability of Elektron services to just that IP address. With this option selected, the "Enable IP Version 6 Services" option is disabled. You may enter either an IPv4 or IPv6 address here regardless of the IPv6 checkbox setting.

Primary Server Port

Elektron allows you to select the UDP port on which it will provide services. Since Elektron provides RADIUS service, by default it listens for incoming connections on the standard RADIUS port 1812. If you change this port, you will also need to reconfigure your wireless access points to talk to Elektron on the new port.

Secondary Server Port

Some legacy equipment uses UDP port 1645 for RADIUS. If you have any such

equipment, you can enable this option to allow Elektron to listen on both ports for incoming RADIUS requests.

License

The License panel allows you to view and change your Elektron serial number.

Serial Number

This is the serial number that you received when you purchased Elektron or requested an evaluation license. If you are moving from an evaluation serial number to a full, purchased license, enter your new serial number here.

If you are using an evaluation serial number, the expiration date of the license is displayed and a button that links to our web site is present to allow you to purchase the full, non-expiring version.

Configuring Clients 5

This chapter shows you how to configure the built-in clients on Windows XP and Mac OS X 10.3.

Windows XP

WPA Enterprise security is an integral component of Windows XP. Configuring wireless networking settings on Windows XP can be difficult; this section attempts to make it a little easier.

System Requirements

You should have Windows XP Service Pack 2 installed. Service Pack 1 also supports WPA Enterprise, but the configuration interface is somewhat different. This section describes the interface for Service Pack 2. You will also need a wireless adapter (such as a PC card) that supports the Windows Wireless Zero Configuration Service (WZC). Most popular wireless adapters sold today are WZC compatible..

Installing the Elektron Certificate

In order to securely configure a Windows XP client for use with your Elektron server, you will need to install your Elektron digital certificate on the client machine. It is possible to configure the Windows XP client to connect to a secure WPA network without validating this digital certificate, but we strongly recommend that you avoid this option.

To install the digital certificate on the client machine:

1. Export the certificate from Elektron using the Elektron Settings application: from the Identity page, use the Windows installer export option.

2. Copy the installer to the client machine by either burning the installer to a CD or placing it on a USB keychain flash drive and transporting the CD or keychain drive to the client machine.

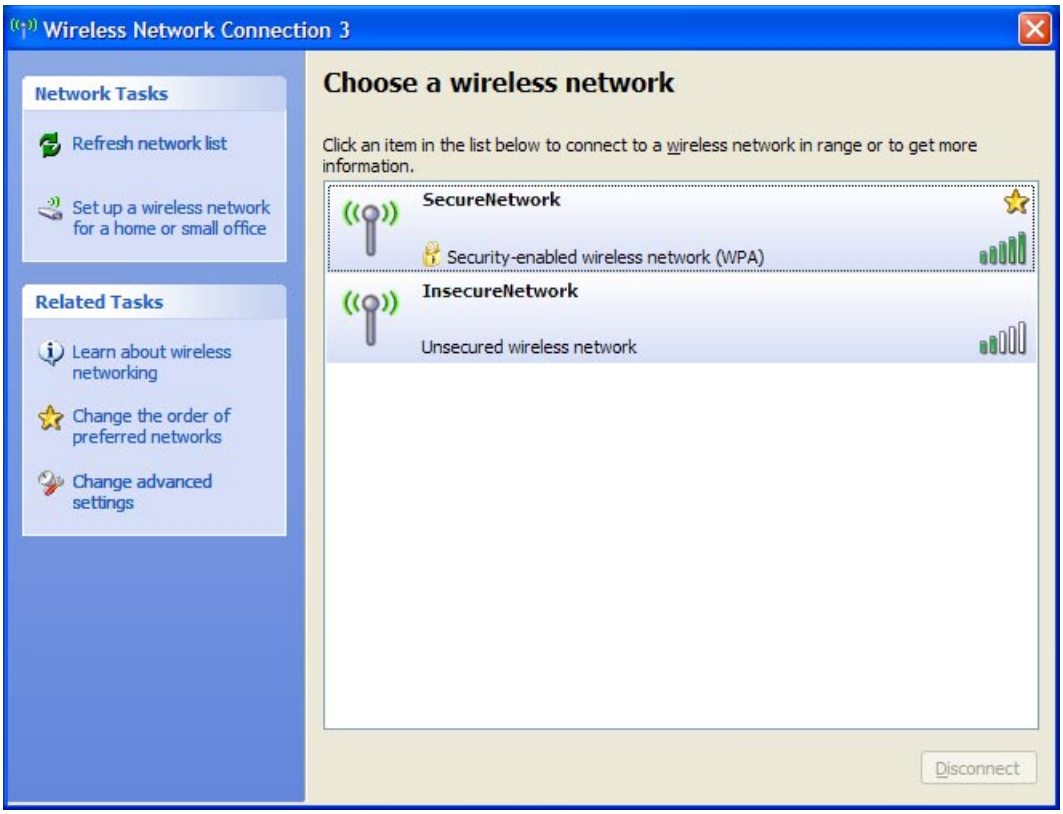
3. Double click the installer and follow the wizard steps to install the certificate.

Selecting Your Network

Once the digital certificate is installed, configuration of the Windows XP client can begin. To configure the client machine to connect to your secure Wi-Fi network:

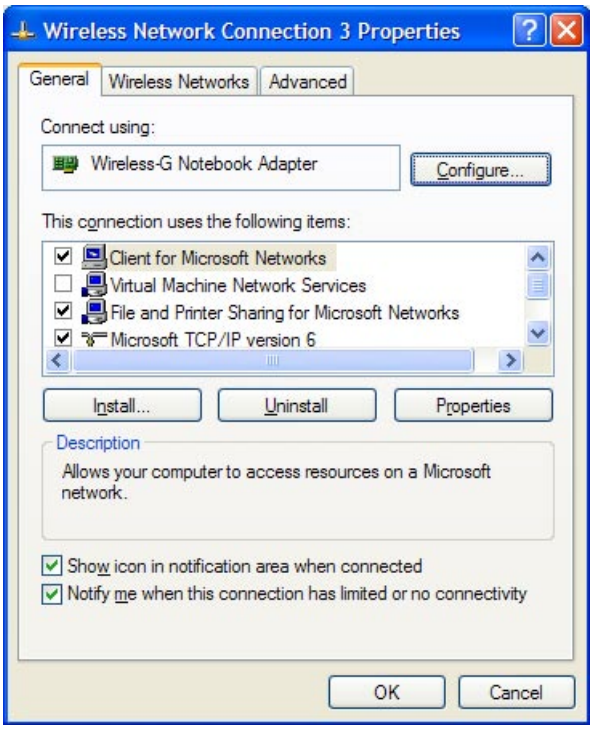
1. From the Start menu select Start->Control Panel. Open the Network Connections folder, and select your wireless connection (usually called "Wireless Connection"). Right click "Wireless Connection" and select "Properties". If there is no item named "Wireless Connection", either your wireless adapter is not installed or there is a problem with its driver.

2. Selecting "Wireless Connection" properties brings up the "Choose a wireless network" dialog:

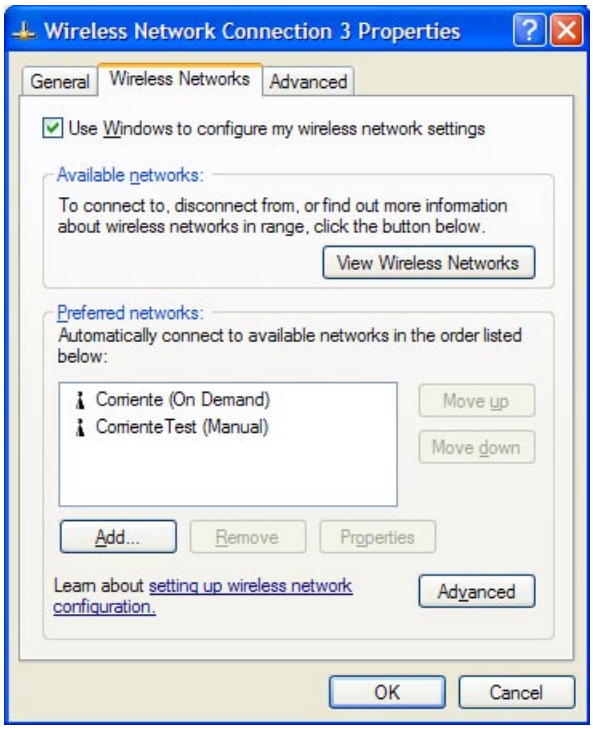


3. From the this dialog, you can select and connect to your network; but don't do so just yet. There are some options that need to be configured before you continue. Note that you won't see your network listed if your access points are configured not to broadcast their SSID (i.e., you create a "closed network" when you configured the access points).

4. Click the "Change advanced settings" link on the left-hand side of the dialog. This brings up the "Wireless Network Connection Properties" dialog:

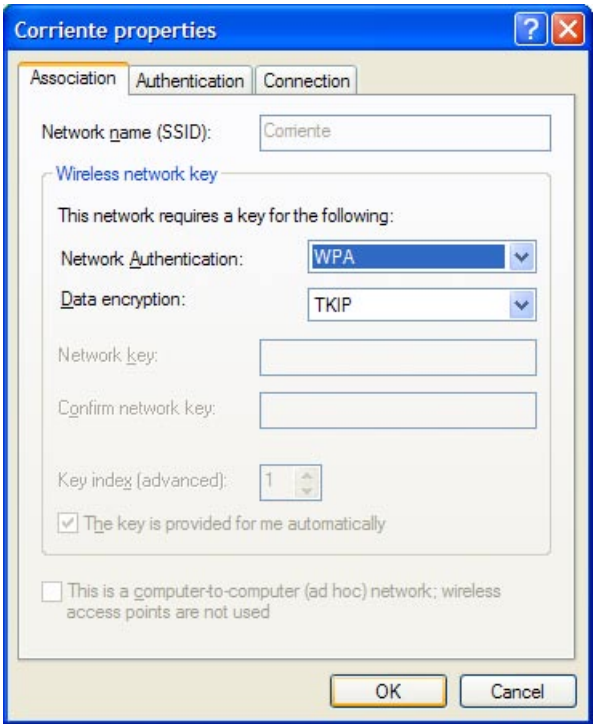


5. Click on the "Wireless Networks" tab. Make sure that "Use Windows to configure my wireless network settings" is checked:

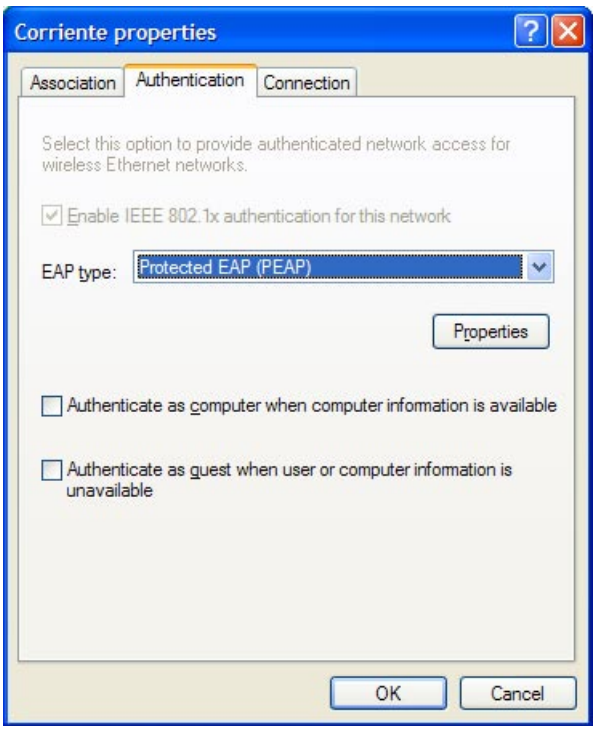


6. In the "Preferred Networks" group, select your network from the list and click "Properties". If your network is not in the list, click "Add..." and enter your network name in the "Network Name (SSID)" field.

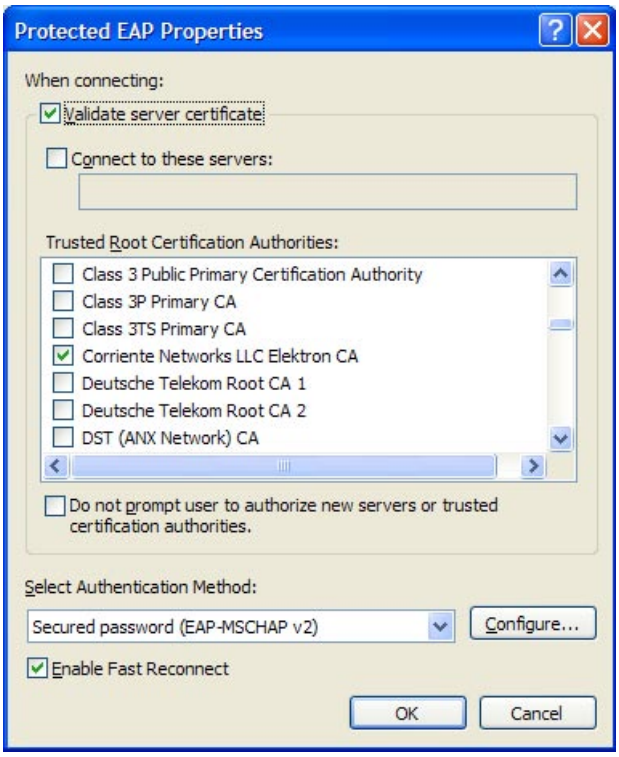
7. On the Association tab, select "WPA" from the Network Authentication pop-up. For Data Encryption, select "TKIP" (you may also select "AES" if computer's wireless adapter and your network's access points all support AES):



8. Click the Authentication tab. Select "Protected EAP (PEAP) as the EAP type. Make sure that "Authenticate as computer when computer information is available" and "Authenticate as guest when user or computer information is unavailable" are both unchecked:



9. After selecting "Protected EAP (PEAP)" as the EAP Type, click the Properties button:



10. If you installed your Elektron digital certificate as described above, check the "Validate server certificate" box and scroll through the Trusted Root Certificate Authorities" list and check the box next to your Elektron certificate name, which will be of the form "<your organization name> Elektron CA". Keep the "Connect to these servers" and "Do not prompt user to authorize new servers or trusted certification authorities" unchecked.

11. If you did not install your Elektron digital certificate, you may uncheck the "Validate server certificate" check box. We recommend that all clients validate the server certificate to ensure the highest level of security.

13. Select "Secured password (EAP-MSCHAP v2)" as the Select Authentication Method, and check the "Enable Fast Reconnect" box. Click OK to close the Protected EAP Properties dialog.

14. Click OK to accept the changes on the Authentication page, and click OK to close the Wireless Network Connection Properties dialog.

Windows client setup can be simplified if you are configuring more than one machine. In Windows XP Service Pack 2, Microsoft introduced the Wireless Network Setup Wizard, which allows you to configure one client machine, and then copy that configuration to other clients without having to manually re-enter all the

configuration information. The Wizard is at Start->Accessories->Communications ->Wireless Network Setup Wizard.

If you choose to use the Wireless Network Setup Wizard, you should install the Elektron digital certificate on the target client machine before copying the configuration. The Wizard does not copy the digital certificate, only the configuration settings that point to it.

Mac OS X

Apple began to include a WPA Enterprise client with Mac OS X 10.3, meaning that no third party software is necessary for Mac OS X 10.3 clients to join and Elektron-protected Wi-Fi network.

System Requirements

To use the Mac OS X client, you must have Mac OS X 10.3 (Panther) or later and an AirPort or AirPort Extreme card. Be sure that the client is running the latest version of the AirPort software by running the Software Update application. AirPort software updates are also available at Apple's AirPort support web site, at:

http://www.apple.com/support/

On Demand Configuration

The easiest way to configure a Mac OS X client is to perform no initial configuration at all. Simply select your Elektron-protected network's name from the system wide AirPort menu (which is present if you have the "Show AirPort status in menu bar" option selected in the Internet Connect application) or by selecting "Other..." from the AirPort menu and typing your network's name (if you have created a closed network). You may also select the network from the AirPort pane in the Internet Connect application.

Entering a Password

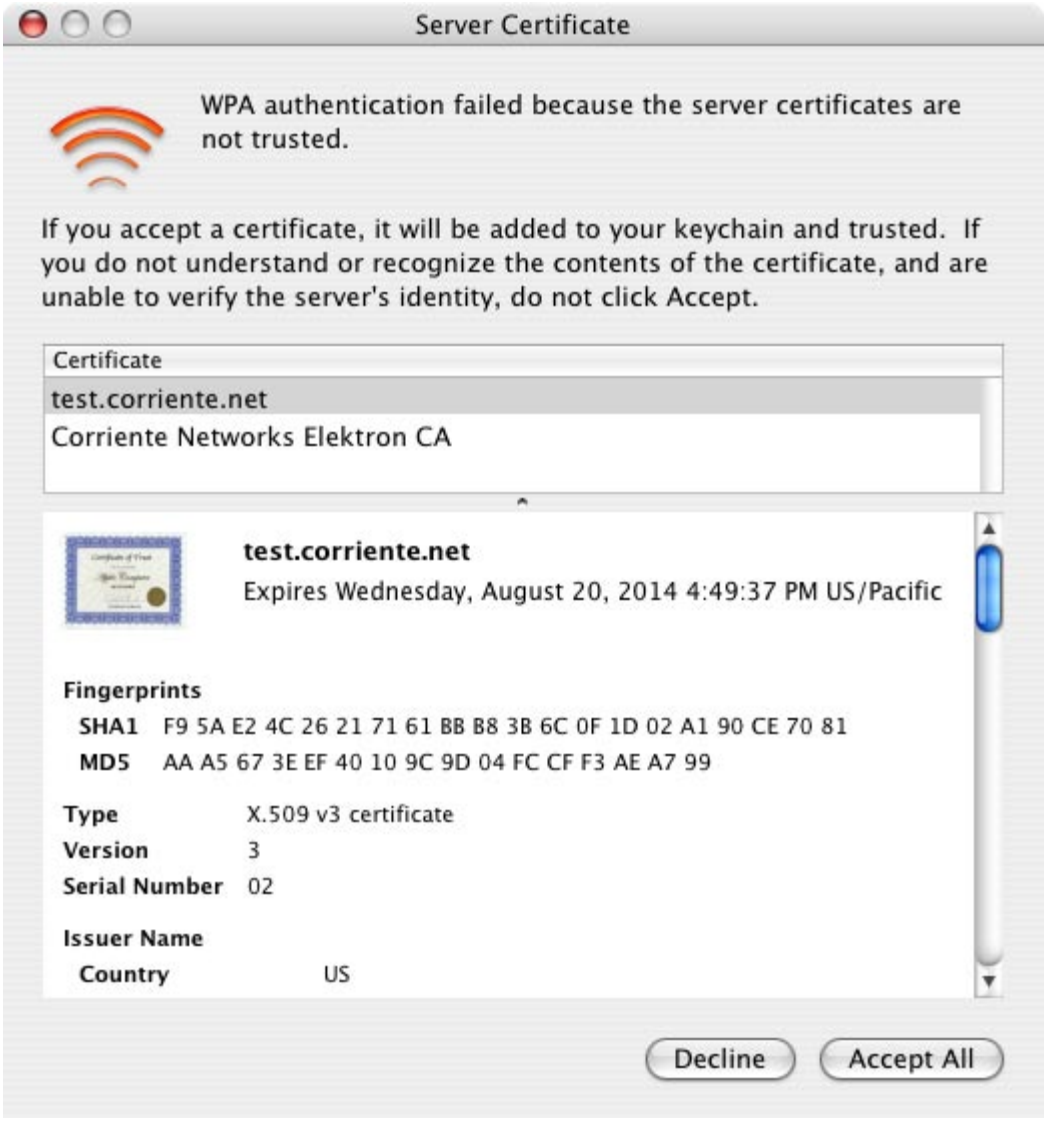
The Mac OS X client software will recognize that your are attempting to login to a WPA Enterprise network, and prompt you for a username and password:

Enter the user's username and password. If Elektron is configured to use system accounts for user authentication (which is the default), then the username and password will be the same as those used by the user to login to the machine on which Elektron is running.

Certificate Authentication

If this is the first time the user has logged into the network, and the Elektron digital certificate has not been previously installed on the user's computer (this optional installation is described later in the chapter), then Mac OS X displays a dialog warning that it does not recognize the server's digital certificate:

Click the "View Certificates" button to review and approve the Elektron digital certificate:



By clicking the "Accept All" button, you are telling Mac OS X that you trust this digital certificate and are willing to connect the network. Before clicking, the certificate needs to be verified. After clicking "Accept All", the login proceeds, and if the username and password were correctly entered, the user will be logged in and able to securely use network services.

Verifying the Certificate

Accepting the server's digital certificate without first verifying it can be dangerous. An attacker may have lured the user into connecting to a rogue network access point and presented the user with their own, untrustworthy certificate. Fortunately, verifying the certificate is easy.

The digital certificate is verified by matching its "fingerprint". A certificate fingerprint is a secure hash (a mathematical computation that distills a block of data

into a series of digits). To begin, you will need the legitimate fingerprint of the server's certificate. This is available in the Elektron Settings application:

1. Launch the Elektron Settings application (located in /Applications)
2. Select the Certificates pane from the toolbar at the top of the window
3. Double-click on the name of your certificate from the Active list
4. The certificate's details are shown. One of the details is the fingerprint:

5. Verify that this fingerprint matches the fingerprint shown by the Mac OS X client (in this example, the fingerprint, "F9 5A E2 4C 26 21 71 61 BB B8 3B 6C 0F 1D 02 A1 90 CE 70 81", matches the fingerprint shown in the client dialog). The colons and spaces displayed in the fingerprint by Elektron and Mac OS X are not part of the fingerprint; they are just there to make it easier to read.

With the certificate verified and the "Accept All" button clicked, the connection is complete. The user is now logged in and ready to use the network.

Full Configuration

To avoid having to manually verify the Elektron digital certificate, Mac OS X clients can pre-install the certificate on their machine. There are two ways to do this:

Certificate Installer Elektron can create a double-clickable installer for Mac OS X clients. Launch the Elektron Settings application, and from

the Identity panel click the "Mac OS X" button. This will allow you to save a package containing the Elektron certificate, which, when opened by the user, will launch the Mac OS X Installer application. You can burn this Installer package to a CD or copy it to a keychain USB flash drive for distribution to clients.

You can customize the Installer package for your users by changing the text that appears on the second pane. To do this, right click "Elektron Certificate.pkg" and select "Show Package Contents" from the contextual menu. Open the Contents folder, then inside the Contents folder, open the Resources folder. The file "ReadMe.txt" contains the text that appears on the installer's second pane. You customize this with information specific to your network. The file is a Rich Text Format (RTF) file than can be edited using TextEdit.

Certificate File

Mac OS X recognizes certain file extensions as files containing digital certificates, including ".pem". When a user double-clicks one of these files in the Finder, Mac OS X will automatically launch the Keychain Access application and give the use the option of adding the certificate to a keychain of the user's choice.

To export your Elektron certificate as an importable file, open the Elektron Settings application and navigate to the Identity panel. Click the "Text File" button to save the file.

When the user receives the file containing the certificate, double-clicking the file (assuming that it has a correct file extension such as ".pem") will result in the Keychain Access application being launched and a keychain dialog being presented:

Select the "X509 Anchors" keychain (if there is more than one X509 Anchors keychain listed, select the one that follows "system" in the menu). This will place the certificate in the correct keychain for the Mac OS X WPA software to find it for verification.

Beyond configuring the certificate, Mac OS X offers users advanced options to select which authentication method is used to verify a client's identity. These are available in the Internet Connect application on the 802.1X pane. To select an authentication method:

1. Open the Internet Connect application
2. If there is no 802.1X pane, select "New 802.1X Connection..." from the File menu
3. Select the 802.1X pane
4. Choose "Edit Configuration..." from the Configuration pop-up menu
5. Check or uncheck the protocols you wish to enable or disable. We recommend PEAP and TTLS be enabled for use with Elektron.
6. Click TTLS in the list to select it and click the Configure button
7. For TTLS Inner Authentication, select PAP, click OK
8. Click OK