How to Use 802.1X on HP Jetdirect Print Servers

May 2008

Table of Contents:

hp

Introduction	2
What is 802.1X?	6
Public Key Infrastructure and Public Key Certificate Basics	7
What Equipment is Required for 802.1X?	15
Installing the Internet Authentication Service (IAS)	
Installing a Certificate Authority (CA)	18
Creating a Certificate Template	24
Issuing a Certificate	30
Creating a User for HP Jetdirect	37
Switch Configuration	40
HP Jetdirect Certificate Configuration	41
IAS Configuration	48
HP Jetdirect 802.1X Configuration	57
Understanding Certificate Chains	61
Utilizing the Server ID Field on Jetdirect	66
Wireless and 802.1X	72
ProCurve Switches and Identity Driven Management	74
Summary	74
Appendix A: Troubleshooting 802.1X	75
Appendix B: Importing a Certificate	88



Introduction

In many organizations, the properties assigned to a user determine the rights they have on the network. For example, some generic user types are shown in Figure 1 – User Types:



Figure 1 - User Types

An Authorized User is a user that has authenticated to the network and been given authorization to access certain resources. An Unauthorized User is a user that was unable to be authenticated and is placed in a network where they can do no harm. A Guest is a user that has been authenticated and given restricted privileges. These users can connect in a variety of ways: dial-in, VPN using broadband, wireless in a conference room, and through a direct connection to a switch as shown in Figure 2 – Connection Types.



Figure 2 - Connection Types

In many cases, the connection type determines what attempts are made to authenticate and authorize users. For example, a wireless connection or dial-in connection may require more stringent credentials than a wired connection. For wired networks, unfortunately, Authorized Users, Unauthorized Users, and Guests may have network access to the same equipment because no authentication and authorization is being done. Uncontrolled access can cause problems – for example, an Authorized Server with a security vulnerability can be exploited by an Unauthorized User. Instead, we would like the wired network architecture to help us isolate equipment to those users that require access to it. Virtual LANs are a common way to accomplish this isolation. See Figure 3 – Virtual LANs.



Figure 3 - Virtual LANs

In Figure 3, independent switches that are each responsible for a single VLAN are used. Each VLAN is for a particular type of user. There is typically a one-to-one correspondence between a VLAN and an IP Subnet. Inter-VLAN communication is routed.

There are a couple of problems with this approach: (1) it doesn't really make sense to have an Unauthorized User VLAN for wired connection and (2) an Unauthorized User can simply plug their computer into the Authorized VLAN switch to circumvent security. It is also very inefficient to dedicate one switch to one VLAN. We could use a single switch and create Port-Based VLANs – for example,

ports 1 through 8 are always assigned to a specific VLAN – but as before, security can be circumvented simply by attaching a computer to the desired port.

For Port-Based VLANS, what we really need are three separate solutions: (1) A way to authenticate users, (2) A way to grant authenticated users access to the network, and (3) A way to assign authenticated users to specific VLANs with network access restrictions, bandwidth constraints, and other controls. A Port-Based VLAN solution with dynamic authentication is shown in Figure 4 – Dynamic VLANs.



Figure 4 - Dynamic VLANs

Here, users are dynamically authenticated and assigned to specific VLANs regardless of what switch port they use. A user that cannot be authenticated is assigned a VLAN where they can do no damage. This behavior is fine for users, but what about printers and MFPs? Well, the nice part about 802.1X is that wired HP Jetdirect print servers support it. All we need to do is create users in Active Directory that correspond to Jetdirect-based printers and printer management servers, and we can do what is shown in Figure 5 – Printing and Imaging VLANs.



Figure 5 – Printing and Imaging VLANs

As shown in Figure 5, printers and MFPs become full-fledged authenticated users of the network and are assigned parameters that help them participate in the security and protection of the network and its resources. This whitepaper will discuss IEEE 802.1X Port Access Control, in relation to printing and imaging environments.

What is 802.1X?

IEEE 802.1X Port Access Control is a generic framework that allows infrastructure devices to control an end-node's access to the network. From an Ethernet perspective, we can refer to Figure 6 – 802.1X Switch Port, and see the breakdown of the Ethernet switch.



Figure 6 - 802.1X Switch Port

The end-node device must authenticate itself to the network before the local switch will grant it access to the network. The end-node device has a valid link to the switch, but the only frames the switch will forward from the end-node to the network are 802.1X Extensible Authentication Protocol (EAP) frames. The technical terminology for the devices involved is shown in Figure 7 – 802.1X Terms.



Figure 7 - 802.1X Terms

In reality, the authenticator (switch) repackages 802.1X EAP frames from the Supplicant and sends them to an Authentication Server. Based upon the configuration in the Authentication Server and the information supplied by the Supplicant, the Supplicant is authenticated (or not). The result of this authentication determines whether the switch port is "opened up" to the network for the Supplicant to send/receive non-EAP frames for normal network operation. With HP ProCurve switches, the Authentication Server can return much more information, such as the VLAN the Supplicant should be assigned, bandwidth restrictions on the Supplicant, etc., and the switch dynamically configures itself to support those parameters.

Because Extensible is part of the name of EAP, there are multiple protocols that have been developed under the EAP framework. All HP Jetdirect products supporting 802.1X also support Protected EAP or PEAP. Many HP Jetdirect products also support EAP-Transport Layer Security or EAP-TLS. These two EAP flavors are the most popular for wired 802.1X deployments. Both protocols utilize SSL/TLS running under EAP to authenticate the Authentication Server which sets up a secure tunnel. When shopping on the Internet, SSL/TLS is often used to protect the transaction over the network and to establish trust that the web site being contacted is really that web site and not an imposter's web site.

A cornerstone of trust in SSL/TLS is the digital certificate. For PEAP and EAP-TLS, the Authentication Server sends over a digital certificate which the supplicant will attempt to validate. After a series of checks are performed, the supplicant will need to establish that the digital certificate was created by a trusted authority. If it passes that test, an SSL/TLS tunnel can be established. At this point, PEAP and EAP-TLS diverge. PEAP uses the tunnel to securely pass credentials via another protocol, typically a username and password, to the Authentication Server while EAP-TLS uses a client digital certificate for authentication. Because how digital certificates are created and validated, we will need to cover them in depth.

Public Key Infrastructure and Public Key Certificate Basics

Have you ever seen the warning dialog shown in Figure 8 when using <u>https://</u> (e.g., going to any secure web site, such as a login or shopping cart) in a web browser?



Figure 8 – Security Alert

This dialog is entitled "Security Alert" and it talks about something called a "security certificate". What is a security certificate?

NOTE: A security certificate, digital certificate, public key certificate, and identity certificate are different terms which all refer to the same thing in this whitepaper.

Well, a security certificate is there to help identify the web site as one that can be trusted. However, the Security Alert dialog is telling us that we may not want to trust this security certificate – which indirectly means that this web site may not be the web site we think it is. There are two warning icons associated with this dialog. The help text by the first warning icon prompts us to view the certificate. Let's click on "View Certificate".



Figure 9 – Certificate Details

In Figure 9, we see there is a red X on the certificate, indicative of a security problem. In addition, there is a very specific error message: "This certificate cannot be verified up to a trusted certification authority." Here we see that the "Issued By" is entitled "RootCA". What the message is trying to say is that "RootCA", who issued the certificate "635n", is not trusted.

A useful analogy is to think of the certificate issuer like a Department of Motor Vehicles (DMV). Each state in the United States has a DMV run by the state's government. The DMV issues driver's licenses which grant the privilege to drive in a given state. A person that goes to the DMV to get a driver's license must pass a series of tests that helps the DMV determine if they are fit to drive on the state's roads. The state's Highway Patrol, a group which enforces the rules of the road, recognizes the validity of the DMV to issue driver's licenses. Therefore, if one violates one of the rules of the road and is pulled over by a Highway Patrol officer, showing a driver's license issued by the DMV is a requirement. The Highway Patrol will not recognize a driver's license issued by an institution other than the DMV as being valid. In short, the DMV is a trusted third party that issues "certificates" (driver's licenses) to individuals. These "certificates", issued by the DMV, are trusted by the Highway Patrol.

The Security Alert dialog is troubling because it is indicative of a trust problem. In the terms of our analogy, it would be like a driver, who has been pulled over by the Highway Patrol, handing the officer a driver's license that the driver's mother wrote for him indicating that her son had been granted the privilege to drive in the state. While a note from mom may be trusted by her sister, it isn't trusted by the Highway Patrol.

In essence, a digital certificate, one used by computers, binds an identity to a key and needs to be issued by a trusted third party. What is a key? A key is a secret that is used in cryptographic algorithms. There are public keys and private keys used for asymmetric cryptography and symmetric keys used for symmetric cryptography. Let's look at symmetric cryptography first.



Figure 10 – Symmetric Cryptography

In Figure 10, the confidentiality provided to the message is done via a single key. Because the same key is used for encryption and decryption, this process is known as symmetric cryptography. Symmetric cryptography commonly has two attributes associated with it:

- It performs well it is fast and easy to implement
- It has a key distribution problem how do you get the symmetric key to everyone that needs it in a secure way?

Asymmetric cryptography is also available and functions very different than symmetric cryptography. It has two keys – one Public and one Private. The private key is not shared with anyone. The Public key is like a public telephone number. You can share it with everyone. Let's look at Figure 11 – Asymmetric Cryptography.



Figure 11 – Asymmetric Cryptography

Here we can see the difference between asymmetric and symmetric cryptography. One key can be used for encryption and then the corresponding key can be used for decryption. It appears that asymmetric cryptography has solved the key distribution issue; however there are two new attributes usually associated with asymmetric cryptography

- It is slow
- It has a trust problem. How do I know that this is John's public key and not someone pretending to be John?

To solve the first problem, asymmetric cryptography is usually used to securely distribute symmetric keys and sign hash codes. In short, what is actually being encrypted and decrypted is usually much smaller than actual messages. This has the nice benefit of solving the key distribution issue with symmetrical cryptography. So, in essence, symmetric keys are sent securely using asymmetric cryptography and the actual messages themselves are protected using symmetric cryptography. Cool! We get the flexibility of asymmetric cryptography and the speed of symmetric cryptography. Now we only have to solve the trust problem.

In order to solve the trust problem, five things will need to be discussed:

- A certificate authority a trusted third party that creates digital certificates from certificate requests
- A certificate request a public key associated with identity information that will serve as the basic building block for a digital certificate that the certificate authority will create and sign.
- A digital certificate a public key associated with identity information that is digitally signed by the certificate authority.
- A digital signature the hash of the digital certificate encrypted by the private key of the certificate authority.

A hash – also known as a message digest. A hash is the output of a one way function that attempts to ensure the integrity of the message (i.e., that the message has not been altered). It is usually combined with authentication information to ensure that the message originator can be authenticated and that the integrity of the message has not been disrupted. You can think of a hash like an advanced checksum or an advanced cyclic redundancy check (CRC).

Let's cover hashes and digital signatures first. We'll assume that Jack wants to send John a message. Jack wants to make sure that John knows the message came from him and that the message was not altered in transit. However, Jack doesn't care about confidentiality – in other words, the actual message can be sent "in the clear" – but does care about authentication and integrity. We can accomplish this through hashes and digital signatures as shown in Figure 12.



Figure 12 – Digital Signature

In Figure 12, Jack has sent John a message with a digital signature. Let's see how John would validate this message to make sure it came from Jack and was not altered. Refer to Figure 13.



Figure 13 – Digital Signature Verification

Here we see how John uses Jack's public key to verify the message. Jack's public key is the only key that can decrypt the digital signature and obtain the hash value of the message that Jack calculated before sending the message. Because the hash was encrypted with Jack's private key, which no one should know but Jack, John can be sure that Jack was the one that sent it.

We still have a problem – How does John know that Jack's public key really belongs to the person that he knows as "Jack"? There are many people in the world named "Jack" – how does John know it isn't one of them? We still need a trusted third party to provide Jack's public key in a format John can trust and we probably need Jack to provide a little more identity information too. Here is where the Certificate Authority comes into play. Refer to Figure 14 – Certificate Authority.



Figure 14 – Certificate Authority

Jack goes through a key pair generation process and creates a public and private key pair. The private key is kept secret. The public key is associated with some identity information and is given to a Certificate Authority. The certificate authority generates a certificate, usually specific to a purpose such as email, and signs the certificate with its digital signature. Assuming there is a place where these digital certificates are publicly available, as long as Jack and John can agree to trust a specific certificate authority, they'll be fine trusting certificates signed by that authority. Refer to Figure 15.



Figure 15 – Public Key Certificates

Here we can see that everyone's public key certificate is, well – um, public. The important thing to note is that the certificate authority also has a public key certificate that identifies itself. This certificate is signed with its own private key and is a "self-signed" certificate. There is no "higher" level of trust then the top level certificate authority. Therefore, John and Jack must choose a particular certificate authority that they both trust. In most cases, there is a hierarchy of certificate authorities at customer sites. This forms what is known as a certificate chain and there is a top level CA or Root CA where the ultimate trust resides.

Also, we should take care to point out that there is usually a difference between Internet trust using certificates and Intranet trust using certificates. Internet trust will involve well-known certificate authorities like Verisign and Entrust. However, Intranet models usually revolve around Microsoft's certificate authority that comes with Windows 2003 server. Each company establishes their own Public Key Infrastructure (PKI) that includes an entire policy around certificates.

Now that we have covered some basics around certificates, we can talk specifically about Jetdirect. Jetdirect is an embedded system and as a result, has limited storage space for certificates. Jetdirect

can store one Identity certificate and one CA certificate. The CA certificate tells Jetdirect which identity certificates should be trusted (i.e., must be signed by that CA) when Jetdirect is receiving a certificate from another entity. Jetdirect's Identity certificate is the certificate that is sent out when another entity requests it. It is important to note that the CA certificate on Jetdirect is configured strictly to provide the trust point for identity certificates that are sent to Jetdirect – the identity certificates received from other entities must be signed by that CA or be part of a chain which ends in that CA.

Since Jetdirect only has one Identity certificate that can be configured, it must be capable of being used in a variety of situations. Jetdirect can act as a client or a server, depending on the protocol being used. For instance, if a web browser is using HTTPS to communicate to Jetdirect, Jetdirect will return its Identity certificate as part of the SSL/TLS negotiation process, which will identify Jetdirect as a server. In other cases, like EAP-TLS, Jetdirect will send its Identity certificate for client authentication.

By default, Jetdirect will create a "self-signed" certificate the first time it is powered on. This certificate is not secure because it has not been signed by a trusted CA. An important step in the security of a Jetdirect product is to replace the default self-signed Identity certificate with one that has been signed by a trusted CA.

What Equipment is Required for 802.1X?

Essentially, we need the following:

- A printer or Jetdirect device (Supplicant) that supports 802.1X
- A switch (Authenticator) that supports port-based authentication via 802.1X
- A RADIUS server (Authentication Server), such as the Internet Authentication Service (IAS) from Microsoft

Many HP Jetdirect devices can be upgraded for free to support 802.1X. Refer to <u>http://www.hp.com/go/webjetadmin_firmware</u> for the latest firmware updates. HP Jetdirect products that support 802.1X are as follows:

- J7934A/J7934G 620n EIO 10/100TX Print Server with the latest firmware available PEAP Support
- J7960A/J7960G 625n EIO 10/100/1000T Print Server with the latest firmware available PEAP support
- J7997G 630n EIO 10/100/1000T Print Server with the latest firmware available PEAP & EAP-TLS support
- J7961A/J7961G 635n EIO IPv6 & IPsec Print Server with the latest firmware available PEAP & EAP-TLS support
- J8007G 690n EIO Wireless 802.11b/g Print Server PEAP & EAP-TLS & LEAP support
- Embedded Jetdirect products with the latest firmware available PEAP & EAP-TLS support
- J7942A/J7942G en3700 USB External Print Server with the latest firmware available PEAP support.

Microsoft's IAS comes with Windows Server 2003. This means that two of the three items needed for 802.1X authentication are potentially free! All that is needed is the switch (Authenticator). Ethernet switches have long supported 802.1X. Check your switch documentation for information on whether or not it is supported. The HP ProCurve line of edge devices support 802.1X with higher-end edge switches supporting rich methods of assigning VLANs, bandwidth constraints, access control lists, etc. Refer to http://www.hp.com/go/procurve

Rather than generically explain what is necessary to setup and configure 802.1X for HP Jetdirect, this whitepaper will go through a step-by-step tutorial of sample installations and configurations of the 802.1X components.

NOTE: The following sections describe in detail the various steps to use 802.1X. Various software programs are installed and configured. The installation and configuration of these programs, such as Microsoft's Certificate Authority, are done for learning purposes and should not be considered as HP's recommended configurations or installations for production networks.

Installing the Internet Authentication Service (IAS)

Where are we	e?
Step 1	Installing Internet Authentication Service
Step 2	Installing a Certificate Authority
Step 3	Creating a Certificate Template
Step 4	Issuing a Certificate
Step 5	Creating a User for HP Jetdirect
Step 6	Switch Configuration
Step 7	HP Jetdirect Certificate Configuration
Step 8	IAS Configuration
Step 9	HP Jetdirect 802.1X Configuration

Microsoft ships a RADIUS server by default. This RADIUS server must be installed from the Add/Remove Windows component wizard.

Using	Windows Components Wizard	×
Windows 2003, we can simply go to	Windows Components You can add or remove components of Windows.	
the Control Panel and select "Add/Remove	To add or remove a component, click the checkbox. A shaded b part of the component will be installed. To see what's included in Details. <u>C</u> omponents:	ox means that only a component, click
then select	Management and Monitoring Tools	6.3 MB 🔺
Mindowa	🖾 🚍 Networking Services	2.7 MB
Composite	🗹 🚔 Other Network File and Print Services	0.0 МВ 🔜
Components.	🗆 🚐 Remote Installation Services	2.0 MB
	🗖 📾 Bernote Storage	35MB 🔟
	Description: Contains a variety of specialized, network-related se Total disk space required: 16.0 MB Space available on disk: 3364.7 MB	rvices and protocols.
	< <u>B</u> ack <u>N</u> ext> C	Cancel Help

Select	Networking Services	
Networking		
Services and	of the component will be installed. To see what's included in a	component, click Details.
oress Details.		
Then select	Subcomponents of Networking Services:	
nternet	🗆 📮 Domain Name System (DNS)	1.7 MB 📥
Authentication	🔲 🛃 Dynamic Host Configuration Protocol (DHCP)	0.0 MB
Service and	🗹 畏 Internet Authentication Service	0.0 MB
oress OK.	🔲 🔲 📇 Remote Access Quarantine Service	0.1 MB
Complete the	RPC over HTTP Proxy	0.0 MB
wizard and	🗆 🌉 Simple TCP/IP Services	0.0 MB
allow the	🔲 🔲 🖳 Windows Internet Name Service (WINS)	0.9 MB 💌
nstallation to :omplete.	Description: Enables authentication, authorization and accounters. IAS supports the RADIUS protocol. Total disk space required: 4.1 MB Space available on disk: 146249.2 MB	inting of dial-up and VPN <u>D</u> etails
		OK Cancel

Installing a Certificate Authority (CA)

Where are we?

Step 1	Installing Internet Authentication Service
Step 2	Installing a Certificate Authority
Step 3	Creating a Certificate Template
Step 4	Issuing a Certificate
Step 5	Creating a User for HP Jetdirect
Step 6	Switch Configuration
Step 7	HP Jetdirect Certificate Configuration
Step 8	IAS Configuration
Step 9	HP Jetdirect 802.1X Configuration

Using Windows 2003 Enterprise Edition or Windows Server 2003 Datacenter Edition, we can simply go to the Control Panel and select "Add/Remove Programs" and then select Windows Components.

	Windows Components Wizard	
elect Certificate ervices", pen click	Windows Components You can add or remove components of Windows.	
lext.	To add or remove a component, click the checkbox. A shad part of the component will be installed. To see what's include Details.	ed box means that only ed in a component, click
	Components:	
	🗹 📻 Accessories and Utilities	4.9 MB 🔺
	Application Server	33.4 MB 💻
	🗹 😰 Certificate Services	1.4 MB
	🗹 🛄 E-mail Services	1.1 MB
	Eax Services	7.9 MB 🔟
	Description: Installs a certification authority (CA) to issue cert public key security programs.	ificates for use with
	Total disk space required: 17.7 MB	Details
	Space available on disk: 3402.7 MB	
	<back next=""></back>	Cancel Help

In this	Windows Components Wizard
example, we are installing an Enterprise Root CA.	CA Type Select the type of CA you want to set up.
Click Next. NOTE: If you select any other kind of CA, the certificate template functionality described below will not be available.	 Enterprise root CA Enterprise subordinate CA Stand-alone root CA Stand-alone subordinate CA Description of CA type The most trusted CA in an enterprise. Should be installed before any other CA.
Here is our CA identity information. Click Next	< Back
and complete the installation.	Common name for this CA: RootCA Distinguished name suffix: DC=example,DC=local Breview of distinguished name: CN=RootCA,DC=example,DC=local Validity period: Expiration date: 11/17/2010 1:58 PM
	< <u>Back</u> <u>Next></u> Cancel Help

Once the installation has completed, we can go to Start -> $\ensuremath{\mathsf{Run}}$ -> $\ensuremath{\mathsf{mmc}}$



At this point, we want to load in separate Snap-Ins into the Microsoft Management Console (MMC). Snap-Ins are modules that provide specific management functionality to the MMC. Go to the File menu and select "Add/Remove Snap-In".



Select	Certification Authority
"Local Computer"	
Then click	Select the computer you want this snap-in to manage.
Finish.	This snap-in will always manage:
	Local computer: (the computer this console is running on)
	C Another computer:B_rowse
	Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.
	< Back Finish Cancel
Select OK	Add/Remove Snap-in
	Standalone Extensions Use this page to add or remove a standalone Snap-in from the console. Snap-ins added to: Console Root Certificate T emplates Certification Authority (Local)
	Add

Done.	Console1
	Elle Action View Favorites Window Help
	The Console Root
	Console Root Name Name
	B D Certification Authority (Local)

Creating a Certificate Template

Where are we? Step 1 Installing Internet Authentication Service Installing a Certificate Authority Step 2 Step 3 Creating a Certificate Template Step 4 Issuing a Certificate Step 5 Creating a User for HP Jetdirect Step 6 Switch Configuration HP Jetdirect Certificate Configuration Step 7 IAS Configuration Step 8 HP Jetdirect 802.1X Configuration Step 9

The Certificate Authority needs to have a template from which certificates can be created for services. The Microsoft CA has some predefined templates to help the administrator. Microsoft also allows you to create new templates. We will illustrate a process of creating a certificate template specifically for an HP Jetdirect print server.

Note: The certificate template functionality described below is only available for Windows 2003 Enterprise Edition and Windows 2003 Datacenter Edition.

Select	Console1 - [Console Root\Certificate Ter	nplates]				
Certificate	E Lie Action Yew Pavgrices Window ← → E III III III E E	Неф				그리스
Templates.	Console Root	Template Display Name A	Minimum Supported CAs	Version	Autoenrollment	
	Certification Authority (Local)	49 Administrator	Windows 2000	4.1	Not allowed	
		Contracted Session	Windows 2000	3.1	Not allowed	
		G Exchange	Windows 2000 Windows Server 2003, Ep.	106.0	Not allowed	
Hiahliaht the		39 CEP Encryption	Windows 2000	4.1	Not allowed	
<i>"</i>		29 Code Signing	Windows 2000	3.1	Not allowed	
"Web Server"		Computer	Windows 2000	5.1	Not allowed	
		Cross Certification Authority	Windows Server 2003, En	105.0	Not allowed	
template, Right I		Directory Email Replication	Windows Server 2003, En	115.0	Allowed	
		Domain Controller	Windows 2000	4.1	Not allowed	
click and copy		Domain Controller Authentication	Windows Server 2003, En	110.0	Allowed	
		EFS Recovery Agent	Windows 2000	6.1	Not allowed	
the certificate		Enrollment Agent	Windows 2000	4.1	Not allowed	
		Enrollment Agent (Computer)	Windows 2000	5.1	Not allowed	
template and		Exchange Enrollment Agent (Offline request)	Windows 2000	4.1	Not allowed	
iempiaie, and		Exchange Signature Only	Windows 2000	6.1	Not allowed	
name it "HP		Exchange User	Windows 2000	7.1	Not allowed	
		Light IPSec	Windows 2000	8.1	Not allowed	
latdiract"		IPSec (Offline request)	Windows 2000	7.1	Not allowed	
Jeidhech .		Key Recovery Agent	Windows Server 2003, En	105.0	Allowed	
Now right click		RAS and IAS Server	Windows Server 2003, En	101.0	Allowed	
NOW HIGHLENCK		29 Root Certification Authority	Windows 2000	5.1	Not allowed	
an "UD		Univer (Offline request)	Windows 2000	4.1	Not allowed	
on Hr		1299 Smartcard Logon	Windows 2000	6.1	Not allowed	
latalina at″ anal		Util Smartcard User	Windows 2000	11.1	Not allowed	
Jetairect and		Utility Subordinate Certification Authority	Windows 2000	5.1	Not allowed	
1 1		Lega Irust List Signing	Windows 2000	3.1	Not allowed	
select		Ligguser	windows 2000	3.1	Not allowed	
			Windows 2000	4.1	Not allowed	
properties.		Web Server	Windows 2000	101.0	Allawed	
				10110		

Provide the	Properties of New Template	
names you	Issuence Deminements Supercoded Templetes Enterprises Convitu	
would like the	General Beguest Handling Subject Name	
certificate		
template to	Template display name:	
have.	HP Jetdirect	
	Minimum Supported CAs: Windows Server 2003, Enterprise Edition	
	After you apply changes to this tab, you can no longer change the template	
	name.	
	Template name:	
	HPJetdirect	
	Validity period: <u>R</u> enewal period:	
	2 years 💌 6 weeks 💌	
	Publish certificate in Active Directory	
	Do not automatically reenroll if a duplicate certificate exists in Active	
	Directory	
	OK Cancel Apply	
Select the	Properties of New Template	
Select the "Allow private	Properties of New Template	
Select the "Allow private key to be	Properties of New Template ? × Issuance Requirements Superseded Templates Extensions Security General Request Handling Subject Name	
Select the "Allow private key to be exported"	Properties of New Template ? × Issuance Requirements Superseded Templates Extensions Security General Request Handling Subject Name	
Select the "Allow private key to be exported" checkbox in the	Properties of New Template ? × Issuance Requirements Superseded Templates Extensions Security General Request Handling Subject Name Purpose: Signature and encryption ▼	
Select the "Allow private key to be exported" checkbox in the Request Handling tab	Properties of New Template ? × Issuance Requirements Superseded Templates Extensions Security General Request Handling Subject Name Purpose: Signature and encryption • Archive subject's encryption private key	
Select the "Allow private key to be exported" checkbox in the Request Handling tab.	Properties of New Template ? × Issuance Requirements Superseded Templates Extensions Security General Request Handling Subject Name Purpose: Signature and encryption • Archive subject's encryption private key Include symmetric algorithms allowed by the subject	
Select the "Allow private key to be exported" checkbox in the Request Handling tab.	Properties of New Template ? × Issuance Requirements Superseded Templates Extensions Security General Request Handling Subject Name Purpose: Signature and encryption • Archive subject's encryption private key • Include symmetric algorithms allowed by the subject Delete revoked or expired certificates (do not archive) •	
Select the "Allow private key to be exported" checkbox in the Request Handling tab.	Properties of New Template ? × Issuance Requirements Superseded Templates Extensions Security General Request Handling Subject Name Purpose: Signature and encryption • Archive subject's encryption private key Include symmetric algorithms allowed by the subject Delete revoked or expired certificates (do not archive) Minimum key size: 1024	
Select the "Allow private key to be exported" checkbox in the Request Handling tab.	Properties of New Template ? × Issuance Requirements Superseded Templates Extensions Security General Request Handling Subject Name Purpose: Signature and encryption • Archive subject's encryption private key • Include symmetric algorithms allowed by the subject Delete revoked or expired certificates (do not archive) • Minimum key size: 1024 • Allow private key to be exported • •	
Select the "Allow private key to be exported" checkbox in the Request Handling tab.	Properties of New Template ? × Issuance Requirements Superseded Templates Extensions Security General Request Handling Subject Name Purpose: Signature and encryption • Archive subject's encryption private key Include symmetric algorithms allowed by the subject Delete revoked or expired certificates (do not archive) Minimum key size: 1024 Image:	
Select the "Allow private key to be exported" checkbox in the Request Handling tab.	Properties of New Template ? × Issuance Requirements Superseded Templates Extensions Security General Request Handling Subject Name Purpose: Signature and encryption • Archive subject's encryption private key • Include symmetric algorithms allowed by the subject Delete revoked or expired certificates (do not archive) • Minimum key size: 1024 • Allow private key to be exported • • Do the following when the subject is enrolled and when the private key associated with this certificate is used: •	
Select the "Allow private key to be exported" checkbox in the Request Handling tab.	Properties of New Template ? × Issuance Requirements Superseded Templates Extensions Security General Request Handling Subject Name Purpose: Signature and encryption • Archive subject's encryption private key Include symmetric algorithms allowed by the subject Delete revoked or expired certificates (do not archive) Minimum key size: 1024 Allow private key to be exported Do the following when the subject is enrolled and when the private key associated with this certificate is used: Enroll subject without requiring any user input	
Select the "Allow private key to be exported" checkbox in the Request Handling tab.	Properties of New Template ? × Issuance Requirements Superseded Templates Extensions Security General Request Handling Subject Name Purpose: Signature and encryption • Archive subject's encryption private key • Include symmetric algorithms allowed by the subject Delete revoked or expired certificates (do not archive) • • Minimum key size: 1024 • ✓ Allow private key to be exported • Do the following when the subject is enrolled and when the private key associated with this certificate is used: • ✓ Enroll subject without requiring any user input • ✓ Prompt the user during enrollment •	
Select the "Allow private key to be exported" checkbox in the Request Handling tab.	Properties of New Template ? × Issuance Requirements Superseded Templates Extensions Security General Request Handling Subject Name Purpose: Signature and encryption • Archive subject's encryption private key Include symmetric algorithms allowed by the subject Delete revoked or expired certificates (do not archive) Minimum key size: 1024 Allow private key to be exported Do the following when the subject is enrolled and when the private key associated with this certificate is used: Erroll subject without requiring any user input Prompt the user during enrollment Prompt the user during enrollment and require user input when the private key is used	
Select the "Allow private key to be exported" checkbox in the Request Handling tab.	Properties of New Template ? X Issuance Requirements Superseded Templates Extensions Security General Request Handling Subject Name Purpose: Signature and encryption Image: Signature and encryption Image: Signature and encryption Image: Archive subject's encryption private key Image: Image: Image: Signature and encryption private key Image: Image: Image: Signature and encryption private key Image: Image: Image: Image: Image: Signature and encryption Image: Signature and encryption private key Image: Image: Image: Signature and encryption private key Image: Image: Image: Image: Image: Image: Image: Signature and encryption private key Image:	
Select the "Allow private key to be exported" checkbox in the Request Handling tab.	Properties of New Template Image: Superseded Templates Extensions Security Issuance Requirements Superseded Templates Extensions Security General Request Handling Subject Name Purpose: Signature and encryption Image: Signature and encryption Image: Archive subject's encryption private key Image: Ima	
Select the "Allow private key to be exported" checkbox in the Request Handling tab.	Properties of New Template ? × Issuance Requirements Superseded Templates Extensions Security General Request Handling Subject Name Purpose: Signature and encryption • Archive subject's encryption private key Igclude symmetric algorithms allowed by the subject Delete revoked or expired certificates (do not archive) Minimum key size: 1024 Vallow private key to be exported Do the following when the subject is enrolled and when the private key associated with this certificate is used: Prompt the user during enrollment Prompt the user during enrollment Prompt the user during enrollment and require user input when the private key is used To choose which cryptographic service providers CSPs) should be used, click CSPs.	
Select the "Allow private key to be exported" checkbox in the Request Handling tab.	Properties of New Template ? × Issuance Requirements Superseded Templates Extensions Security General Request Handling Subject Name Purpose: Signature and encryption • Archive subject's encryption private key Include symmetric algorithms allowed by the subject Delete revoked or expired certificates (do not archive) Minimum key size: 1024 Allow private key to be exported Do the following when the subject is enrolled and when the private key associated with this certificate is used. Enroll subject without requiring any user input Prompt the user during enrollment Prompt the user during enrollment and require user input when the private key is used To choose which cryptographic service providers (CSPs) should be used, click CSPs.	
Select the "Allow private key to be exported" checkbox in the Request Handling tab.	Properties of New Template ? X Issuance Requirements Superseded Templates Extensions Security General Request Handling Subject Name Purpose: Signature and encryption • Archive subject's encryption private key Include symmetric algorithms allowed by the subject Delete revoked or expired certificates (do not archive) Minimum key size: 1024 Image: Allow private key to be exported Do the following when the subject is enrolled and when the private key associated with this certificate is used: Image: Prompt the user during enrollment Prompt the user during enrollment and require user input when the private key is used To choose which cryptographic service providers (CSPs) should be used, click CSPs. Image: OK Cancel Apply	

Select the	Properties of New Template
Application	General Request Handling Subject Name
Policies	Issuance Requirements Superseded Templates Extensions Security
extension in the	To modify an extension, select it, and then click Edit.
Extensions tab.	
Click Edit.	Extensions included in this template:
	Certificate Template Information Issuance Policies Key Usage
	Edit
	Server Authentication
	An application policy defines how a certificate can be used.
	Application policies:
	Server Authentication
	Add Edit <u>B</u> emove
	Make this extension critical
	OK Cancel

Select Client	Add Application Policy	? ×
Authentication,	An application policy (called enhanced key usage in Windows 2000)	
then click OK.	defines how a certificate can be used. Select the application policy re for valid signatures of certificates issued by this template.	quired
	for valid signatures of certificates issued by this template.	
	Application policies:	
	Certificate Bequest Agent	
	Client Authentication	
	Lode Signing Digital Rights	
	Directory Service Email Replication	
	Embedded Windows System Component Verification	
	Encrypting File System	
	IP security end system	
	IP security IKE intermediate	
	IP security user	-
	New	. 1
	OK Cano	
Click OK.	Edit Application Policies Extension	
	An application policy defines how a partificate can be	
	used.	
	Application policies:	
	Client Authentication	
	Server Authentication	
	Add Edit Remove	
	I Make this extension critical	
	OK Cancel	

Click OK.	Properties of New Template
	General Request Handling Subject Name
	Issuance Requirements Superseded Templates Extensions Security
	To modify an extension, select it, and then click Edit.
	Extensions included in this template.
	Key Usage
	Description of Application Policies:
	Client Authentication
	OK Cancel Apply

Now we have created a new certificate template, we need to enable it to be used by the Certification Authority.



Select HP	🔲 Enable Certificate Ten	nplates			<u>?×</u>
Jetdirect and	Select one or more Certifica	ate Templates to enable	on this Certification Authority		
click OK.			en une connocation national		
	Name		Intended Purpose		
	Code Signing		Code Signing		
	Cross Certification Aut	hority	<all></all>		
	Enrollment Agent		Certificate Request Agent		
	Enrollment Agent (Cor	nputer)	Certificate Request Agent		
	Exchange Enrollment	Agent (Offline request)	Certificate Request Agent		
	Exchange Signature (Dnly	Secure Email		
	Exchange User		Secure Email		
	HP Jetdirect		Server Authentication, Client Au	thentication	
	IPSec		IP security IKE intermediate		
	IPSec (Offline request)	IP security IKE intermediate		
	Keu Becoveru ågent		Keu Recoveru årient		<u> </u>
				ОК	Cancel
	*** Console1 - [Console Doot) Certification	Authority (Local)\ BootCA\ Certi	ficate Templates]		
View the	Elle Action View Favorites Window	/ <u>H</u> elp	neace remplaces]		
Certificate					
Templates	Console Root	Name	Intended Purpose		
folder in the	Certification Authority (Local)	Directory Email Replication	Server Authentication, Client Auther Directory Service Email Replication	tication	
	Revoked Certificates	Domain Controller Authenticat	ion Client Authentication, Server Auther	nticatio	
Certification	Issued Certificates	Basic EFS	Encrypting File System		
Authority snap-	Failed Requests	Domain Controller	Client Authentication, Server Auther Server Authentication	tication	
in MMC, and	Certificate Templates	Computer	Client Authentication, Server Auther	ntication	
		User Subordinate Certification Auth	Encrypting File System, Secure Emai ority <all></all>	, Clien	
make sure that		Administrator	Microsoft Trust List Signing, Encrypti	ng File	
the HP Jetdirect					
template is					
ionipiane ie					
present.					
Done.					
		1			
		1			
		1			
				1	J

Issuing a Certificate

Installing Internet Authentication Service		
Installing a Certificate Authority		
Creating a Certificate Template		
Issuing a Certificate		
Creating a User for HP Jetdirect		
Switch Configuration		
HP Jetdirect Certificate Configuration		
IAS Configuration		
HP Jetdirect 802.1X Configuration		

We need to download the CA certificate for Jetdirect and make sure our client know about the CA chain as well.

From the main	Microsoft Certificate Services - Microsoft Internet Explorer Joi X Elie Edit View Favorites Tools Help
web interface	🔇 Back 🔹 🔿 👻 😰 🏠 🔎 Search 👷 Favorites 🕜 🔗 🔹 🗟
click	Address 🗿 http://loopback/certsrv/
"Download a	Microsoft Certificate Services RootCA Home
CA	Welcome
cennicale	Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks. You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. For more information about Certificate Services, see <u>Certificate Services Documentation</u> . Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL

Select "Current		
[RootCA]″.	Microsoft Leftificate Services - Microsoft Internet Explorer File Edit View Favorites Tools Help	
then DFR (or	😮 Back 🔹 🕑 👻 🖹 🙎 🏠 🔎 Search 👷 Favorites 🛷 😥 😓	
Base 64 if you	Address 🗃 http://loopback/certsrv/certcarc.asp	Links »
aro using an	Manager Cartificate Samiras DestCA	Hama
alder latdirect	Microson Centricate Services - Routica	TOME
	Download a CA Certificate, Certificate Chain, or CRL	
product), then	To trust certificates issued from this certification authority, install this CA certificate chain.	
	To download a CA sortificate partificate shain or CDL select the sortificate and encoding method	
Download	To download a CA certificate, certificate chain, of CRL, select the certificate and encoding method.	
CA	CA certificate:	
certificate",	Current (RootCA)	
	Encoding method:	
	© DER © Base 64	
	Download CA certificate	
	Download CA certificate chain	
	Download latest date CRL	
		-
	Done	1.

Click Save.	File Download - Security Warning
	Do you want to open or save this file?
	Name: certnew.cer Type: Security Certificate, 1.10 KB From: loopback Open Save Cancel
	While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. <u>What's the risk?</u>



We also want to install the CA certificate chain on the local computer. This will allow the browser to recognize certificates issued by the CA as trusted.

	A Microsoft Certificate Services - Microsoft Internet Evolorer
Click "Install	File Edit View Favorites Tools Help
this CA	🕜 Back + 😧 - 🖹 😰 🏠 🔑 Search 🤹 Favorites 🛷 🔗 - 😓 🚍
	Address 🕘 http://loopback/certsrv/certcarc.asp
	×
chain".	Microsoft Certificate Services RootCA <u>Home</u>
	Download a CA Certificate, Certificate Chain, or CRL
	To trust certificates issued from this certification authority, install this CA certificate chain.
	To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.
	CA certificate:
	Current (RootCA)
	Encoding mathed
	C Base 64
	Download CA certificate
	Download CA certificate chain
	Download latest delta CRI
	· · · · · · · · · · · · · · · · · · ·
	🝘 Install this CA certificate chain 👘 👘 Internet
Click Vee	
Click Tes.	Potential Scripting Violation
	This Web site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web
	site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data.
	Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.
	<u>Y</u> es

	A Microsoft Certificate Services - Microsoft Internet Explorer	اد
9	Ele Edit View Favorites Iools Help	
	🔾 Back 🔹 🕘 👻 😰 🏠 🔎 Search 🤹 Favorites 🕐 🙆 🌜 🚍	
	Address 🙆 http://loopback/certsrv/certrmpn.asp	r 🛃 Go Lin
	Microsoft Certificate Services RootCA	Home
	CA Certificate Installation	
	The CA certificate chain has been successfully installed.	
		have a b
	Me Done	rernet

Now we can begin creating an Identity Certificate for Jetdirect. Starting with Jetdirect firmware version V.36.11 and later, certificates created from CSRs and issued by the Enterprise CA can be installed. This method is a more secure way (and preferred way) of installing a certificate. If your HP Jetdirect firmware is earlier than V.36.11 (e.g., V.29.20, V.31.08), please refer to Appendix B for instructions on how to import a certificate. First, we need to create a CSR on Jetdirect.

Click on the "Networking" tab and go to "Authorization" and then "Certificates". Click "Configure" under the Jetdirect	Information Settings Digital Configuration TCPAP Settings TCPAP Settings Network Settings Other Settings Settings Privacy Settings Security Settings Settings Authorization Mgmt. Protocols 802.1X Authorization Psec/Firewall Diggnostics Network Statistics Protocol Info Configuration Page	I Sending Networking Authorization Support I Admin. Account Certificates Access Control Certificates are used to identify devices on the network: Jetdirect Certificate By default, a pre-installed self-signed Jetdirect certificate is created to identify Jetdirect. You can change this certificate to more accutely identify the device and to update the length of time the certificate is valid. Status: Installed View Configure CA Certificate Accertificate is required for some authentication methods. It is used to verify the authentication server's certificate. Status: Installed View Configure
Certificate section.		-

Certificate	Configuration	Authorization	Support ?			
Request" and then click "Next".	Network Settings Other Settings	Certificate Options				
	Privacy Settings Security Settings	An X.509 certificate is required by various sec may create a certificate request. A self-signer does not provide trusted authentication of the certificate. You may also inport a certificate a	surity protocols. You may update the pre-installed self-signed certificate, or you I certificate provides encryption of data between the client and device, however it device. Data encryption and trusted authentication is provided by a third party on private kerk upsa as the lefticed certificate or you may export the existing the second the second term of t			
	Authorization	Jetdirect certificate and optionally its private key.				
	Mgmt. Protocols 802.1X Authentication	C Create New Self-Signed Certificate	Create a new self-signed certificate. Warning: This operation will overwrite the currently installed certificate with a new self-signed certificate.			
	Psec/Firewall Diagnostics Network Statistics Protocol Info	Create Certificate Request	Create the Certificate Request that you will give to a Certificate Authority. The Certificate Request will be used to generate a certificate for you.			
		C Import Certificate and Private Key	Import a certificate and private key to use as the Jetdirect certificate. (Note: This will overwrite the current Jetdirect certificate and private key.			
	Configuration Page	C Export Certificate	Export the Jetdirect certificate and private key.			
			Next > Cancel			

lds that	Configuration TCP/IP Settings	Authorization	Support ?
describe the devices. Click "Next".	Network Settings Other Settings Privacy Settings Security	Certificate Information	
		Please specify the following values to uniquely identify the certificate. The Certificate A accuracy and completeness to ensure that the certificate is being issued to a legitimate	uthority will check the fields for organization.
	Settings Authorization	Caution: You are now creating a new certificate request. By doing so, you will be erasing any existing request.	
	Mgmt. Protocols 802.1 X Authentication IPsec/Firewall Diagnostics Network Statistics	Common Name Fully qualified domain name or IP Address of the Jetdirect finance device.	xe.example.internal
		Organization Full legal name of your company. Do not abbreviate, except for Examp Inc., Corp, etc. (Ex: Hewlett-Packard Co.)	ole
		Organizational Unit Specific department or division within your organization. Printin (optional)	g
	Protocol Info	City/Locality City in which your organization is physically located.	
	Configuration Page	State/Province State in which your organization is physically located.	
		Country/Region Two-character ISO 3166 country/region code. (Ex: "us" for USA).	

Jetdirect generates the public/private key pair, which can take a little while.	Digital Sending Networking Support 2 Configuration Result STATUS: Certificate request creation in progress. This may take up to 3 minutes without a screen update.
Network Statistics Protocol Info Configuration Page	










We are going to use this file to Import into Jetdirect as well as associated a certificate with an Active Directory user.

Creating a User for HP Jetdirect

Where die we.	
Step 1	Installing Internet Authentication Service
Step 2	Installing a Certificate Authority
Step 3	Creating a Certificate Template
Step 4	Issuing a Certificate
Step 5	Creating a User for HP Jetdirect
Step 6	Switch Configuration
Step 7	HP Jetdirect Certificate Configuration
Step 8	IAS Configuration
Stop 0	

Where are we?

Using Windows 2003, we can simply go to the Start Menu, Select Administrator Tools, then select "Active Directory Users and Computers". Highlight the Users folder and create a generic user. If we are going to use PEAP, we simply want to specify a password that never expires for the user. This password will be used in the Jetdirect configuration for 802.1X, so it is important to remember it and use strong passwords. If we are going to use EAP-TLS, we need to associate this user with the Identity Certificate configured on Jetdirect.

In Active Directory Users and computers, we want to go to the view menu and make sure "Advanced Features" is checked.	Active Directory Users and Computers Elle Action Sile Action Yew Window Help Add/Remove Columns Large Icons Small Icons Small Icons Wather Director Large Icons Small Icons Users, Groups, and Computers as containers Oronging Advanced Features Domain Users Customize Progration Value (Strengther Computers) Progration (Strengther Computers) Users Oronging Advanced Features Detail Customize Progration (Strengther Computers) Progration (Strengthe	Image: Security Group Members who have view Security Group New brack view Security Group DNS deninistrators Group Security Group DNS clients who are permi Security Group All domain guests Security Group All domain users Security Group All domain guests Security Group Built-in account for guest Security Group Built-in account for guest Security Group Its Worker Process Group User Built-in account for anony User Built-in account for Intern User Built-in account for Intern User Built-in account for anony User Security Group Security Group User Security Group Security Group Security Group Security Group Security Group Security Group Security Group Security Group
Click on the Account tab and make sure that the Account Options has "Password never expires" selected. Enter the Logon name, typically the hostname, of the HP Jetdirect card.	HP Jetdirect Properties Published Certificates Memb Environment Sessions Remote General Address Account User logon name: Implesore Implesore MPIESOT57 User logon name (pre-Windows 2) EXAMPLEN Logon Hours Log Or Account is locked out Account gptions: Implement of the server expires User cannot change password User cannot change password Store password using rever Account expires Implement of the server Store password using rever Implement of the server Implement of the server Store password using rever	Profile Dial-in Object Security control Terminal Services Profile COM+ Profile Telephones Organization @example.local 2000): NPIE80157 In To ord at next logon word In To OK Cancel Apply

Click the Dial-	HP Jetdirect Properties
select "Allow access". Then	Environment Sessions Remote control Terminal Services Profile COM+ General Address Account Profile Telephones Organization Published Certificates Member Of Dial-in Object Security
Click OK.	Remote Access Permission (Dial-in or VPN)
	C Deny access C Control access through Remote Access <u>Policy</u>
	Zerify Caller-ID:
	No Gallback Set by Caller (Routing and Remote Access Service only) Always Callback to:
	Assign a Static IP Address
	Apply Static Boutes Define routes to enable for this Dial-in connection. Static Routes
	OK Cancel Apply

At this point, we will want to associate the public key certificate of the Jetdirect print server with the HP Jetdirect account.



Select "X.509 Certificates" and "Add…" Now using the certificate that	Security Identity Mapping X.509 Certificates Kerberos N. Mapped user account:	ames	<u>?×</u>
the CA issued	example.local/Users/HP Jetd		
"finance cer"	≚-509 certificates:		
was the file	Certificates For	Issued By	
you can map it here. Click "OK".	CN=J7961A 000E7FE8015	. CN=RootCA	
	<u>Add</u> <u>E</u> dit	<u>R</u> emove	
		DK Cancel	Apply

Switch Configuration

Where are we? Step 1 Installing Internet Authentication Service Step 2 Installing a Certificate Authority Creating a Certificate Template Step 3 Step 4 Issuing a Certificate Creating a User for HP Jetdirect Step 5 Switch Configuration Step 6 HP Jetdirect Certificate Configuration Step 7 Step 8 IAS Configuration Step 9 HP Jetdirect 802.1X Configuration

Each Switch (Authenticator) configuration will vary. For this example, we are using an HP J4902A 6108 ProCurve Switch. Essentially, we enable 802.1X for port 8 of the switch and tell the switch where the Radius server is. We haven't installed the Radius server, but we will soon. The switch will relay the EAP messages from Jetdirect to the Radius Server. The Radius server will work with Active Directory to determine if the user can be authenticated. If so, the switch will open up the port and allow Jetdirect access to the network.

Based upon this configuration, the Jetdirect device needs to be installed in Port 8. That is the only port that is enabled for 802.1X. Refer to Figure 16 for an example configuration file.



Figure 16 - Example Switch Configuration

HP Jetdirect Certificate Configuration

Step 1	Installing Internet Authentication Service
Step 2	Installing a Certificate Authority
Step 3	Creating a Certificate Template
Step 4	Issuing a Certificate
Step 5	Creating a User for HP Jetdirect
Step 6	Switch Configuration
Step 7	HP Jetdirect Certificate Configuration
Step 8	IAS Configuration
Step 9	HP Jetdirect 802.1X Configuration

Where are we?

Now we can discuss the HP Jetdirect configuration for 802.1X. First, we will install the HP Jetdirect Certificate and the CA Certificate on the HP Jetdirect device. The HP Jetdirect certificates are used by SSL, IPsec, as well as 802.1X EAP authentication. Because multiple authentication methods use these certificates, we created the certificates using the certificate template to act as both a client and server.

One of the challenges of 802.1X configuration on HP Jetdirect print server is that there is no out-ofband mechanism to configure 802.1X. As a result, we must connect the HP Jetdirect print server to a non-802.1X port first, then configure the 802.1X settings, then move the HP Jetdirect to an 802.1X port on the switch. In order to install HP Jetdirect certificates, the CA certificate, and configure 802.1X, we need to use the Embedded Web Server (EWS).



With the 635n print server, the browser is automatically redirected to use SSL (https://) For other HP Jetdirect products, change the URL to use https:// rather than http:// to ensure that EWS communication is secure. The redirection to SSL requires the HP Jedirect print server to send its default certificate to Internet Explorer. Because each HP Jetdirect print server is shipped with a self-signed certificate, a security alert is issued because the browser cannot determine if the certificate is valid and shows a Security Alert dialog as in Figure 17.



Figure 17 – Security Alert Dialog



Click "Yes" to continue. Once we replace the Jetdirect certificate, the above dialog will change.

At this point,	🖉 169.254.10.225 - Microsoft II	nternet Explorer	
you'll be on the	<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>I</u>	iools <u>H</u> elp	1
"TCP/IP	🔇 Back 🔹 🕤 👻 😰 🐔	🔎 Search 🤹 Favorites 🕐 🎰 🗟	1
Settings" link	Address E https://169.254.10.22	25/ 💌 🔁 Go	Links »
for Jetdirect.	(b) N	PIE80157 / 169.254.10.225	
On the left	invent	HP LaserJet 4050 Series	_
hand	Home	tworking	
navigation			100
menu, select	CONFIGURATION (TCP/IP Settings	TCP/IP Settings	_ 1
"Authorization".	Network Settings	Summary Network Identification TCP/IP(v4) (TCP/IP(v6) Config Precedence Advanced	
	Privacy Settings	Host Name: NPIE80157	
	Select Language		
	SECURITY	IPv4 Status: Enabled Fully Qualified Domain Name(IPv4):	
	Settings Authorization	IPv4 Address:	
	Mgmt. Protocols	Address: 169.254.10.225	
	IPsec	Default Gateway: 169.254.10.225	
	DIACNOSTICS	Config By: Auto IP	
	Network Statistics		100
	Protocol Info Configuration Page	IPv6 Status: Enabled	
		Address Prefix length Config By Valid I fm Prof I fm	
	Other Links 🚽	fe80::20e:7fff:fee8:157 64 Link-Local Infinite Infinite	
		2001:db8:120:0:20e:7fff:fee8:157 64 Router 29d23h58m42s[6d23h58m42s]	<u> </u>
		j j j j j j j j j j j j	//,
Click the		mbarrat Famlanca	
"Certificates"	File Edit View Favorites I	iools Help	
tab.	🔾 Back 🔹 🔿 👻 😰 🐔	🔑 Search 👷 Favorites 🛛 🖉 🖓 🕞	
	Address 🗃 https://169.254.10.22	25/ 💌 🛃 Go	Links »
		PIE80157 / 169.254.10.225	
	invent	HP LaserJet 4050 Series	
	Home	tworking	
	CONFIGURATION TCP/IP Settings	Authorization	
	Network Settings	Admin. Account Certificates Access Control	
	Privacy Settings		
	Select Language	Use the fields below to set or change the Administrator Password. When set, the Administrator Password will be required before you can access and change configuration	
	SECURITY	parameters. To disable the Administrator Password, leave the entries blank.	
	Authorization	Note: You may choose to automatically set the SNMPv1/v2 Set Community Name to the	
	Mgmt. Protocols	Administrator Password, if you use HP web Jeradmin, you will need to provide the Administrator Password as the SNMP Set Community Name.	
	IPsec	User Name: Admin	
	DIACNOSTICS	Password:	
	Network Statistics	Confirm Password:	
	Protocol Info Configuration Page	Use the Administrator Password as the Set Community Name	
			_
	Other Links 🚽	Apply Cancel	
		internet	11.

There are two certificates on HP Jetdirect. One is the HP Jetdirect Identity certificate used for SSL, certain EAP protocols, IPsec, etc... The other is the Certificate Authority (CA) public key certificate which tells HP Jetdirect what CA it is supposed to trust. This CA certificate becomes very important for certain 802.1X EAP methods. Certificates may be exchanged and HP Jetdirect needs to be able to verify the received certificate was signed by the trusted CA. We'll install the CA certificate first.





Now we want to install the Identity Certificate.

TCP/IP Settings	Authorization	Support ?
Network Settings Other Settings	Certificate Options	
Privacy Settings Security Settings Authorization	An X.509 certificate is required by various sec may create a certificate request. A self-signer it does not provide trusted authentication of th certificate. You may also import a certificate a Jetdirect certificate and optionally its private ke	surity protocols. You may update the pre-installed self-signed certificate, or you d certificate provides encryption of data between the client and device, however edvice. Date ancryption and trusted autherficiation is provided by a third partly nd private key to use as the Jetdirect certificate, or you may export the existing ey.
Mgmt. Protocols 802.1X Authentication IPsec/Firewall Diagnostics	C Create New Self-Signed Certificate	Create a new self-signed certificate. Warning: This operation will overwrite the currently installed certificate with a new self-signed certificate.
	C Create Certificate Request	Create the Certificate Request that you will give to a Certificate Authority. The Certificate Request will be used to generate a certificate for you.
Network Statistics Protocol Info	Install Certificate	Install a certificate created for you by a Certificate Authority. (Note: The certificate must have been derived from the last certificate request generated by this interface.)
Configuration Page	C Import Certificate and Private Key	Import a certificate and private key to use as the Jetdirect certificate. (Note: This will overwrite the current Jetdirect certificate and private key.
	C Export Certificate	Export the Jetdirect certificate and private key.
	Network Settings Cher Settings Privacy Settings Security Settings Authorization Mgmt: Protocols 802.1X Authentication Pisso:Firewall Diagnostics Network Statistics Protocol Info Configuration Page	Network Settings Cherrificate Options Other Settings An X.509 certificate is required by various set security Settings An X.509 certificate is required by various set authorization Authorization Authorization Mgmt. Protocols B02.1X Authentication of Protocol Info Diagnostice Create New Self-Signed Certificate Network Statistics Create Certificate and optionally its private key Origunation Page Install Certificate

Select the	Information Settings D	Digital Sending Networking
ertificate file	Configuration TCR/P Settings	Authorization Support 2
aved	Network Settings Other Settings	Install Certificate
reviously.	Privacy Settings	Note: The certificate must have been created using the last Certificate Request generated by this Jetdirect.
Click "Finish"	Security	File Name: trator/Desktop/tinance.cer Browse
	Authorization	
	Mgmt. Protocols 802.1X Authentication IPeec/Frewall Diagnostics Network Statistics Protocol Info Configuration Page	<back cancel<="" finish="" td=""></back>

Configuration	
TCP/IP Settings	Support
Network Settings	
Other Settings	
Privacy Settings	
Security	4
Settings	Configuration Result
Authorization	
Mgmt. Protocols	
802.1X Authentication	The certificate has been successfully installed.
IPsec/Firewall	OK
Diagnostics	
Network Statistics	
Protocol Info	
Configuration Page	

Now we have the files that represent Jetdirect's identity certificate and the public key certificate of the CA we trust. We can setup the IAS server.

NOTE: In later HP Jetdirect firmware versions, when a certificate is installed, you are able to protect the private key by restricting how a certificate can be exported.

IAS Configuration

Where are we	?
Step 1	Installing Internet Authentication Service
Step 2	Installing a Certificate Authority
Step 3	Creating a Certificate Template
Step 4	Issuing a Certificate
Step 5	Creating a User for HP Jetdirect
Step 6	Switch Configuration
Step 7	HP Jetdirect Certificate Configuration
Step 8	IAS Configuration
Step 9	HP Jetdirect 802.1X Configuration

We have installed IAS, but we have not configured it yet. Run the administrator tool for IAS as shown in Figure 18.



Figure 18 – IAS Administration

	🖓 Internet Authentication Service
Here is the	Elle Action View Help
main screen	
for IAS. Vynaf	P Internet Authentication Service (Local) Name Order
we need to do is define the switch as a RADIUS Client.	RADIUS Clients Remote Access Logging Remote Access Policies Connection Request Processing
We know the	
switch that will	New RADIUS Client
be acting as	Name and Address
the	Turne a friendly many and either an ID Address or DNC many far the alignst
Authenticator.	r ype a menuly name and exner an in Address of DNS name for the client.
Input a friendly	Friendly name:
name and the	
IP address of	192.168.0.2 Verifu
Click "Next"	<u></u>
Chek Hexi .	
	· · · · · · · · · · · · · · · · · · ·
	< Back Next > Cancel

Select "Radius	New RADIUS Client
from the drop	Additional Information
down list for "Client- Vendor".	If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client. Client-Vendor:
	RADIUS Standard
To communicate with the radius server, a shared secret needs to be established. Use the same	Shared secret: xxxxx Confirm shared secret: xxxxx Image: Bequest must contain the Message Authenticator attribute
configured on the switch. Click "Finish".	< <u>B</u> ack Finish Cancel

Now that we have a client defined, we can define a Remote Access Policy. Don't let the "Remote Access" terminology confuse you. RADIUS was originally designed to Authenticate Dial-In users – However it has been adapted into a variety of functions – one of these is 802.1X Authentication. Let's go ahead and define a Remote Access Policy for Printing and Imaging Devices. We'll call it PID.

Back to the main screen of IAS, highlight	✓ Internet Authentication Service Eile Action View Help ← → € ● ● ●		
"Remote Access Policies".	Internet Authentication Service (Local) RADIUS Clients Remote Access Logging Remote Access Policies Connection Request Processing	Name There are no items to show	Order

	New	► D	Name	Order
	Refresh Export List		There are no	items to show in this view.

A wizard starts. Click "Next".	New Remote Access Policy Wizard Image: State of the state
	<pre></pre>

Select "Use the					
vitard " and	New Remote Access Policy Wizard				
	Policy Configuration Method				
give the policy	The wizard can create a typical policy, or you can create a custom policy.				
a name. Since					
we are					
detining a	How do you want to set up this policy?				
policy for	Use the wizard to set up a typical policy for a common scenario				
Printing and					
Imaging	 Set up a custom policy 				
Devices, we'll					
call it PID.	Type a name that describes this policy.				
Click "Next".					
	Policy name: PID				
	Europeir Authoritieste all'/IPM connections				
	Example. Autrenidate all VEN connections.				
	Kack Next Cancel				
Select	New Remote Access Policy Wizard				
"Ethernet".					
Click "Next".	Access Method Policy conditions are based on the method used to gain access to the network				
	Select the method of access for which you want to create a policy				
	Selectine method of decess for which you want to credie a policy.				
	O VPN				
	Use for all VPN connections. To create a policy for a specific VPN type, go back to the previous page, and select Set up a custom policy.				
	previous page, and science of up a custom policy.				
	 Use for dialum connections that use a traditional phone line or an Integrated Services. 				
	Digital Network (ISDN) line.				
	C Wireless				
	Use for wireless LAN connections only.				
	Use for Ethernet connections, such as connections that use a switch.				
	< Back Next > Lancel				

ick "Next".	User or Group Access You can grant access to individual users, or you can grant access to selected groups.
	Grant access based on the following:
ect "Smart rd or other tificate".	< Back
ck "Next".	Smart Card or other certificate

Click "Finish".	New Remote Access Policy Wizard
	Completing the New Remote Access Policy Wizard
	You have successfully completed the New Remote Access Policy Wizard. You created the following policy:
	PID
	Conditions: NAS-Port-Type matches "Ethernet"
	Authentication: EAP(Smart Card or other certificate)
	Encryption: Basic, Strong, Strongest, No encryption
	To close this wizard, click Finish.
	< <u>B</u> ack Finish Cancel

Highlight the	PID Properties	1
Highlight the PID policy and right click and bring up the Properties. Select "Grant remote access permission". Press "Edit Profile".	Settings Specify the conditions that connection requests must match. Policy gonditions: Day-And-Time-Restrictions matches "Sun 00:00-24:00; Mon 00:00-24:00; Add Edit Bemove	
	Agd Edit Itentove If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection. Edit Profile Edit Profile Unless individual access permissions are specified in the user profile, this policy controls access to the network. If a connection request matches the specified conditions: O Eny remote access permission If a connection request matches the specified conditions: O K Cancel Apply	

	dit Dial-in Profile
check boxes.	
Press "EAP	Authentication Encryption Advanced
Methods".	
	Select the authentication methods you want to allow for this connection.
	EAP Methods
	Microsoft Encrypted Authentication version 2 (MS-CHAP v2)
	User can change password after it has expired
	Microsoft Encrypted Authentication (MS-CHAP)
	□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □
	Encrypted authentication (CHAP)
	Upencrupted authentication (PAP, SPAP)
	method.
	OK Cancel Apply
Select "Smart	
Card or other	EAP Providers
certificate"	ypes are negotiated in the order in which they are listed.
"Edit"	uper:
"Edit" EAP to	ypes: t Card or other certificate Move Up
"Edit" EAP to Smar Prote	ypes: t Card or other certificate scted EAP (PEAP)
"Edit" EAP to Small	ypes: t Card or other certificate :cted EAP (PEAP) Move Down
"Edit" EA <u>P</u> to Smar	ypes: t Card or other certificate A Move Up Move Down
"Edit" EAP to Smar Prote	ypes: t Card or other certificate A Move Up Move Down Move Down
"Edit" EAP to	ypes: t Card or other certificate socted EAP (PEAP) Move Down
"Edit" EAP to	ypes: tt Card or other certificate scted EAP (PEAP) Move Down
"Edit" EAP to Smart	ypes: t Card or other certificate Acted EAP (PEAP) Move Down Move Down Move Down
"Edit" EAP to Smart	ypes: t Card or other certificate sected EAP (PEAP) Move Down Move Down Move Down

Select the certificate for the machine. Click OK.	Smart Card or other Certificate Properties This server identifies itself to callers before the connection is completed. Select the certificate that you want it to use as proof of identity. Certificate issued to:
	Friendly name:
	Issuer: RootCA
	Expiration date: 11/17/2006 6:47:33 PM
	OK Cancel
Highlight the "Connection Request Policies" and make sure it has "Use Windows authentication for all users".	Internet Authentication Service Image: Service Service Image: Service (Local) Name Processing Order Remote Access Logging Remote Access Dokids Connection Request Policies Remote RADIUS Server Groups

HP Jetdirect 802.1X Configuration

Where are we?

Step 1	Installing Internet Authentication Service
Step 2	Installing a Certificate Authority
Step 3	Creating a Certificate Template
Step 4	Issuing a Certificate
Step 5	Creating a User for HP Jetdirect
Step 6	Switch Configuration
Step 7	HP Jetdirect Certificate Configuration
Step 8	IAS Configuration
Step 9	HP Jetdirect 802.1X Configuration

Up to this point, we have been interfacing with Jetdirect using a non-802.1X port. Once we setup 802.1X on Jetdirect, we will have to move it to an 802.1X port. Based upon our configuration, this is port 8 on the switch. However, once we have specified an 802.1X configuration, it has to be right, otherwise, we will have to Reset the 802.1X configuration from the control panel menu or cold-reset and start over again. Luckily there are only a few fields we need to worry about getting right. Let's look at Jetdirect's 802.1X page in Figure 19 and discuss each field.

ile <u>E</u> dit <u>V</u> iew F <u>a</u> vorites	Tools Help	
Back 🔹 🕘 🖌 💽 🛃	🔎 Search 👷 Favorites 🙆	a• & 🗗
dress 🕘 https://192.168.0.4	1	🗾 🄁 Go 🛛 L
	NPIE80157 / 192.168.0.4 HP LaserJet 4050	Series
Home	Networking	
CONFIGURATION TCP/IP Settings Network Settings	802.1x Authentio	cation
Other Settings Privacy Settings	WARNING: Use caution wh Authentication	en changing the print server's authentication settings; you may lose your connection.
SECURITY	Enable Protocols:	
Settings Authorization	User Name: Password:	INPIE8U15/@example.local
Mgmt. Protocols (802.1x Authentication)	Confirm Password:	
IPsec	Server ID: Encryption Strength:	Require Exact Match
DIAGNOSTICS Network Statistics	Jetdirect Certificate:	Installed Configure
Configuration Page	CA Certificate: Authentication Behavio	Installed Configure
Other Links Help Support		Apply Cancel Restore Defaults

Figure 19 – HP Jetdirect 802.1X Configuration

- **Enable Protocols** Select the EAP method you would like to use. Multiple EAP methods may be selected. When multiple EAP methods are selected, the priority is determined by the Authentication Server when it responds to Jetdirect's EAP Start packet.
- **User Name** This field needs to be the user name of Jetdirect that was configured in Active Directory. Depending on the IAS configuration, you may need to add the realm as well. Adding the realm usually doesn't hurt.
- **Password/Confirm Password**: This is the password for the Jetdirect's user account. These two fields are only needed for PEAP and are not used for EAP-TLS.
- **Server ID**: This field is very important. It relates to the Common Name that is returned in the Subject of the Authentication Server Certificate and determines whether Jetdirect should

accept it. As a good first step in getting 802.1X working, <u>leave this field blank</u> which instructs Jetdirect to match any name that is returned, provided the certificate is trusted.

- **Encryption Strength**: This field determines the minimum strength of the SSL tunnel by determining what ciphers are advertised by the Jetdirect card in the TLS Client Hello packet. By default, it is set to accept Low, Medium, High encryption strengths which correspond to various ciphers and key sizes and allows all of them to be advertised by Jetdirect. A good first step in getting 802.1X working is to leave this field at the default setting.
- **Jetdirect Certificate**: This field simply shows the status of the HP Jetdirect Identity Certificate. It is used only in EAP-TLS.
- **CA Certificate**: This field is used in both PEAP and EAP-TLS. It is extremely important that the Root Certificate Authority is configured so that Jetdirect can determine whether the certificate received from the Authentication Server can be trusted. <u>If this field is not set</u> properly, 802.1X will not work on Jetdirect.

Based upon our example we've been going through so far, let's look at what our 802.1X configuration would be.

Select "802.1x	🖉 192.158.0.4 - Microsoft Tateraet Explorer	×I
Authentication"	Elle Edit View Favorites Iools Help	
from the left	🔾 Back 🔹 🕤 👻 📓 🐔 🔎 Search 👷 Favorites 🛛 🙆 • 🖏 🖂	
hand	Address (2) https://192.168.0.4/	*
navigation	MPIE80157 / 192.168 0.4 HP LaserJet 4050 Series	
menu. Enter		1
the Jetdirect		
logon	CONFIGURATION 802.1x Authentication	
information.	Network Settings	
It's extremely	Privacy Settings Authentication Authentication	
important for	Select Language Enable Protocols:	
the User Name	Settings User Name: NPIE80157@example.local	
format to be	Authorization Password:	
correct, and it	802.1x Authentication Confirm Password:	
needs to match	IPsec Server ID:	
what Active	DIAGNOSTICS Line philon strength. Low (DE3-de-bit, RC4+120-bit of DDE3-18d-bit)	
Directory has	Protocol Info Configuration Page CA Certificate: Installed Configure	
for the Jetdirect	Authentication Behavior: 🔽 Reauthenticate on Apply	
account. Click	Other Links	
"Apply". Now	Help Support Apply Cancel Restore Defaults	
we need to		
move the		
Jetdirect device		
to port 8 of the		
switch, the port		
configured for		
802.1X.		
	le l	
		117

At this point, we want to move our HP Jetdirect to port 8 of the switch. This will force 802.1X authentication to happen. We can review the event log on the system that is running our IAS server to determine whether authentication has been successful or not.

Viewer, under System, 802.1X events will be logged. Double click on an event for IAS.	Image: Section of the section of th	
Here is a successful logon recorded by the event view for our HP Jetdirect device.	Event ? × Date: S/11/2006 Source: IAS Time: 11:12:18 AM Category: None • Type: Information Event [D: 1 User: N/A • Computer: WIN-SERVER Description: User NPIE80157@example.local was granted access. Fully-Qualified-User-Name = example.local/Users/HP Jetdirect NAS-IP-Address = 192.168.0.2 NAS-Identifier = HP ProCurve Switch 6108 Client-Friendly-Name = 6108 Switch Client-IP-Address = 192.168.0.2 Calling-Station-Identifier = 00-0e-7f-e8-01-57 NAS-Port = 8 Proxy-Policy-Name = Use Windows authentication for all users Data: Bytes Words 0000: 00 00 00 00 Master Complexity and the state of the state	

Here we see that the printer was granted access! You can see a Jetdirect configuration page in Figure 20 where EAP-TLS was successful:

🏄 Cannot find server - Micro	soft Internet Explorer				_ 🗆 🗙
<u>Eile Edit View Favorites</u>	<u>I</u> ools <u>H</u> elp				
🔾 Back 🔹 🕤 👻 👔 🔮	🎽 🔎 Search 🛭 👷 Favorites 🛛 🤗 🍰				
Address 🙆 http://192.168.0.2	1/hp/jetdirect			💌 芛 Go	Links »
	NDI765227 / 102 169 0 21				
(A)	he Leger let 1250				
invent	np LaserJet 4350				
Information Settin	Networking				
Information Sector					
CONFIGURATION	Latdina at Calafiau rad	ion Dono			-
TCP/IP Settings	Jetairect Configurat	ion Page			
Network Settings	General Informat	ion	TCP/	IP	
Other Settings	Status:	I/O Card Ready	Status:	Ready	
Privacy Settings					
Select Language	Model Number:	J7949E	II		
Participation and an and an and	Hardware Address: Firmware Version:	V 33 14 FF	IDv4 Domain Name:	NPI/SF33/ example internal	
SECURITY	LAA:	000E7F75F337	Primary DNS Server:	192.168.0.1	
Settings	Port Config:	100TX FULL	Secondary DNS Server:	Not Specified	
Authorization	Auto Negotiation:	On	WINS Server:	Not Specified	
Mgmil, Protocols	Manufacturing ID:	4420442000****	Idle Timeout:	270 sec	
002. IX Muthenucation	Date Manufactured:	05/2004			
DIAGNOSTICS	Security Settin	gs			
Network Statistics	802.1X:	EAP-TLS			
Protocol Info	Admin Password:	Not Specified			
Configuration Page	Secure Web:	HTTPS Optional	IPv	4	
	SNMP Versions.	0-20 23:34 UIC 1.2	IF Address: Subnet Mask.	255 255 255 0	
	SNMP Set Cmty Name:	Not Specified	Default Gateway:	192.168.0.1	
Other Links	Access List:	Not Specified	Config By:	DHCP	
Help			DHCP Server:	192.168.0.1	
HP Home	Network Statist	ics	TFTP Server:	192.168.0.1	
	Iotal Packets Received: Unicast Packets Received:	269	web Jetadmin URL:	Not specified	
	Bad Packets Received:	0	mDNS Service Name:		
	Framing Errors Received:	o	hp LaserJet 4350 [75F	337]	
	Total Packets Transmitted:	334			
	Unsendable Packets:	0			
	Transmit Collisions:	0			
	Transmit Late collisions.	0			
	IPX/SPX		AppleT	alk	
	Status:	Initializing	Status:	Ready	
	Primary Frame Type:	Auto Select	Name: Zone:	hp LaserJet 4350 *	
	Network Frame Type	Revd	Type 1:	HP LaserJet	
			Type 2:	LaserWriter	
			Network Number:	65281	
			Node Number:	4	
			DLC/L	LC	
	Novell/NetWar	e	Status:	Ready	-
ど Done				Internet	1.

Figure 20 – HP Jetdirect 802.1X Success

If there were any issues with authentication, you won't be able to access HP Jetdirect over the network. You can see the failure in the event log. Refer to Microsoft documentation on IAS to troubleshoot any issues with IAS. The configuration of HP Jetdirect, the Switch, and the IAS server must be correct for 802.1X to work properly. It is sometimes useful to get the configuration working with a Windows XP client and test out the infrastructure to make sure all problems are resolved before working with HP Jetdirect. Windows XP can be configured and manipulated without having to use the network. This capability makes troubleshooting easier. With HP Jetdirect, the network must be used to configure 802.1X, which is difficult to troubleshoot when problems arise.

Once HP Jetdirect is configured for 802.1X authentication, 802.1X authentication MUST be successful for any non-802.1X networking activity to occur. If 802.1X authentication is not successful for whatever reason (e.g., switch port doesn't support 802.1X, the 802.1X configuration is wrong, etc...), the networking protocol stacks on HP Jetdirect remain in the initializing state and are not functional. In Figure 21, a Jetdirect configuration page can be seen showing such a state:



Figure 21 – HP Jetdirect 802.1X Failure

In other words, once 802.1X is configured and then fails on an 802.1X port, moving the Jetdirect device to a non-802.1X port is not sufficient to restore network connectivity. Depending on the product, you will either have to "cold-reset" the Jetdirect device or go into the "Security" menu in the Jetdirect control panel menu and select "802.1X", then "Reset", then power down and then power-up. In order for connectivity to be established, Jetdirect will need to be on a non-802.1X port when performing either of those two reset methods.

In Appendix A: Troubleshooting 802.1X, we will cover network trace analysis for HP Jetdirect and some common errors that can be seen and diagnosed through these traces.

Understanding Certificate Chains

The previous example was using a single Certificate Authority that was issuing certificates directly to devices like IAS and Jetdirect. That configuration is uncommon in most customer environments. What is more common is using a hierarchy of Certificate Authorities. This hierarchy can cause some configuration headaches on Jetdirect because of Intermediate Certificate Authorities or Subordinate Certificate Authorities. Let's look at a new example shown in Figure 22.



Figure 22 – CA Hierarchy

In this example, RootCA is the top level CA, which is also called the Root. What usually happens at customer sites is that the Root CA is created and it issues one or more certificates to Subordinate CAs, also known as Intermediate CAs, and they do the dirty work of issuing certificates to various entities in the customer's network. The Root CA is then shutdown and locked up in a secure room with this information backed up in several places. The Root CA establishes the trust of the whole environment and is very well protected.

We can see that RootCA issues a certificate to R2, which grants R2 the capability to issue certificates to other entities. R2's certificate is signed by the Root CA. R2 then can issue certificates to other devices, such as IAS. If we take a look at IAS' certificate, the issuing "chain" or path looks like Figure 23:

Eertification path RootCA RootCA R2 R2	
	View Certificate
rtificate <u>s</u> tatus:	
rtificate <u>s</u> tatus: is certificate is OK.	

Figure 23 – Certification Path

In the certificate itself, there is only one issuer which refers back to R2. We can see that in Figure 24:

Eertifica	ate Information		
This certificate •Proves yo •Ensures th	e is intended for t our identity to a remo he identity of a remo	the following (the computer ote computer	ourpose(s):
Issued to:	: ias.example.inter	nal	
Issued by	r: R2		
Valid from You have a	n 6/29/2007 to 6/: a private key that co	28/2008 rresponds to th	is certificate.
			-

Figure 24 – Issued By

What does R2's certificate look like? We can see it in Figure 25:

This certificate is intended for the following purpose(s): •All application policies Issued to: R2 Issued by: RootCA Valid from 6/29/2007 to 6/29/2009	🚞 Certificate	Information		
Issued to: R2 Issued by: RootCA Valid from 6/29/2007 to 6/29/2009	This certificate is i •All application	intended for the policies	following purpos	ie(s):
Issued by: RootCA Valid from 6/29/2007 to 6/29/2009	Issued to: R	2		
Valid from 6/29/2007 to 6/29/2009	Issued by: R	ootCA		
	Valid from 6/	29/2007 to 6/29/;	2009	

Figure 25 – Issued By

Notice that R2's certificate is issued by RootCA. What does RootCA's certificate look like? Let's look at Figure 26.

This certificate is intended for the following purpose(s): • All issuance policies • All application policies • All application policies Issued to: RootCA Issued by: RootCA Valid from	Certifica	ate Information
Issued to: RootCA Issued by: RootCA Valid from 1/6/2007 to 1/6/2012	This certificate • All issuand • All applicat	e is intended for the following purpose(s): e policies tion policies
Issued by: RootCA	Issued to:	RootCA
Valid from 1/6/2007 to 1/6/2012	Issued by	: RootCA
	¥alid from	1/6/2007 to 1/6/2012

Figure 26 – Issued By

Notice the RootCA is "self-signed". All Root CAs will be self-signed – these CAs represent the single point of trust. A logical question would be: "Which CA do I configure on Jetdirect?" Let's look at some diagrams. First, we have an incorrect configuration, as shown in Figure 27 – Incorrect HP Jetdirect CA Configuration.



Figure 27 – Incorrect HP Jetdirect CA Configuration.

The Subordinate CA cannot be used as the CA certificate on Jetdirect!

Now we can look at a correct configuration in Figure 28 – Correct HP Jetdirect CA Configuration.



Figure 28 - Correct HP Jetdirect CA Configuration

Be sure the Root CA of your CA Hierarchy has its public key certificate configured on Jetdirect!

Utilizing the Server ID Field on Jetdirect

In our first example, we left the Server ID field on Jetdirect blank so that any name in the certificate would match and we could get 802.1X up and running. Once we have succeeded in getting 802.1X up and running, we may want to provide more security by specifying a Server ID. The first thing we need to do is to look at the Authentication Server's certificate that is going to be returned to Jetdirect. In our new example, it is the ias.example.internal certificate shown in Figure 29:



Figure 29 – IAS Certificate

Click on the "Details" tab and go to the "Subject" line as shown in Figure 30.

Series Construction	
Field	Value
	V3
Signature algorithm	61 13 03 88 00 00 00 00 00 00 05
Tssuer	R2, example, internal
Valid from	Friday, June 29, 2007 3:47:25
Valid to	Saturday, June 28, 2008 3:47
Subject	ias.example.internal
Public key	RSA (1024 Bits) 🔹
N = ias.example.internal	

Figure 30 – IAS Subject

Here we can see the Common Name (CN) in the subject field is ias.example.internal. This becomes the value that the server ID field must be configured to match. Before we get into that configuration, it is important to understand another practical deployment procedure used by customers to supply redundancy to their IAS infrastructure. This practice greatly affects the value used in the Server ID field. Refer to Figure 31 for an example of this deployment.



Figure 31 – IAS Redundancy

Usually, the switches are configured to point to both IAS servers in case one is unavailable. Assuming that ias2.example.internal is the Common Name for the second IAS server (in the certificate's Subject field), Jetdirect now can receive one of two names for the Authentication Server

- ias.example.internal
- ias2.example.internal

Jetdirect's Server ID field handles these situations via the following algorithm in Figure 32:



Figure 32 – Server ID Matching

Let's look at some examples that show the behavior of the Server ID field with two IAS servers configured as 802.1X Authentication Servers as shown previously:

- <u>Example 1</u>: Jetdirect Server ID: Blank. Result: If the Authentication Server's certificate is trusted, accept all Common Names returned in the Subject field of the Authentication Server certificate
- <u>Example 2</u>: Jetdirect Server ID: "example.internal", Require Exact Match not checked. Result: If the Authentication Server's certificate is trusted, accept all Common Names returned in the Subject field of the Authentication Server certificate that have "example.internal" as a rightmost subset. "ias.<u>example.internal</u>" and "ias2.<u>example.internal</u>" will both be accepted because "<u>example.internal</u>" is a rightmost match for both.
- **Example 3**: Jetdirect Server ID: "ias", Require Exact Match not checked. Result: If the Authentication Server's certificate is trusted, accept all Common Names where "ias" is a rightmost subset of the name. Here, both servers "ias.example.internal" and "ias2.example.internal" will be REJECTED because it is not a rightmost subset of the name. "ias" is a LEFTMOST match, it is NOT a rightmost match.
- **Example 4**: Jetdirect Server ID: "ias.example.internal", Require Exact Match is checked. Result: If the Authentication Server's certificate is trusted, accept all Common Names where ias.example.internal is the EXACT name. Here, the server ias2.example.internal will be REJECTED because it does NOT match EXACTLY "ias.example.internal"
- **Example 5**: Jetdirect Server ID: "ias.example.internal", Require Exact Match not checked. Result: If the Authentication Server's certificate is trusted, accept all Common Names where ias.example.internal is a rightmost subset of the name. Here, the server ias2.example.internal will be REJECTED because it is not a rightmost subset of the name.

As we can see, Jetdirect's Server ID field allows for fine grained use of which certificate will be accepted and can be configured to support multiple Authentication Servers without accepting all common names.

In Figure 33, we see a proper configuration for this setup (Matching Example 2).



Figure 33 - Correct Server ID For Example 2

In Figure 34, we see an improper setup.

	ternet Explorer
Eile Edit View Favorites	Iools Help 🖊 🦧
🔇 Back 🔹 🔍 👻 😰 🐔	🔎 Search 🤹 Favorites 😧 🍙 💺 🖂
Address Address http://192.168.0.21	/hp/jetdirect 🗾 🖉 Go 🛛 Links 🎽
Information Settin	NPI75F337 / 192.168.0.21 hp LaserJet 4350 gs Networking
CONFIGURATION TCP/IP Settings Network Settings Other Settings Privacy Settings Select Language SECURITY Settings Authorization Mgmt. Protocols (802.1x Authentication DIAGNOSTICS Network Statistics Protocol Info Configuration Page Other Links Help Support HP Home	802. 1x Authentication WARNING: Use caution when changing the print server's authentication settings; you may lose your connection. Authentication Enable Protocols:
Done	Trusted sites
Test in constant for A	Figure 34 - Incorrect Server ID

In Figure 34, the user is trying to match the name IAS. However, this value will result in no matches based upon the Server ID field and the algorithm it uses.

Wireless and 802.1X

The new HP Jetdirect 690n Wireless 802.11b/g EIO card has 802.1X technology too. It also has a wired interface as you can see:



The wired interface makes setting up the wireless interface much easier. In many cases where wireless is used for network printers and MFPs, it is because no wired connection is available. Using a laptop and a direct connection with a LAN cable to the 690n card allows wireless settings and 802.1X to be setup very easy. There are some considerations when setting up a 690n in this way
- Only one network connection can be active at a time. Therefore, once the wireless settings have been configured, unplugging the LAN cable is required so that the wireless interface will be used instead
- When switching from wired to wireless (or vice versa), a reboot is required and is done automatically.
- If you make a mistake on the wireless 802.1X settings and want to use a wired connection to diagnose the problem, you'll need to go into the control panel menu and Reset the 802.1X configuration before plugging in a LAN cable.

Here is the first	Information Settings	Networking
screen of the	Configuration	
wireless setting	Wireless	Wireless Support ?
it continuos	TCP/IP Settings	
	Network Settings	General
in the next	Select Language	WARNING: Use caution when changing the print server's wireless network settings; you may lose your connection.
screen shot	Security	Use the Wireless Wizard to walk you through the configuration of the wireless settings below Wireless Wizard
	Settings	
	Authorization	Network Name (SSID)
	802.1X Authentication	Existing wireless network : hpsetup Refresh
	IPsec/Firewall	O Enter a Network Name :
	Diagnostics	Ad Hoc Network Channel: 10 💌
	Protocol Info	Security
	Configuration Page	No Security
		O WEP
		Authentication : Open
		WEP Key :
		Key index . Key 1 Y Options (1,2,3,4)
		WPA Version : Auto (WPA2 then WPA)
		Authentication : Open
Enterprise is		WEP Key :
selected and		Key Index : Key 1 Options (1,2,3,4) Note: To configure I avaged must be supported by your browner.
the 802.1X		WPA (WFI Protected Access)
configuration		WPA Version : Auto (WPA2 then WPA)
		Encryption : Auto (AES then TKIP)
is about the		WPA - Personal
same as what		
we have been		WPA - Enterprise Note: The 802.1X settings configured here will also be applied to the wired LAN interface.
covering for		Enabled Protocols : LEAP PEAP PEAP. EAP-TLS
wired		User wante . wireless@example.internal
wired.		
		Server ID : Example internal Require Exact Match
		Encryption Strength : Medium (RC4-128-bit or 3DES-168-bit)
		Jetdirect Certificate : Installed Configure
		CA Certificate : Installed Configure
		Authentication Behavior: Reauthenticate on Apply
		NOTE: Only one LAN connection can be active at any time.Printer/MFP will automatically reboot after the LAN cable has been removed from the device in order to connect to the wireless LAN in addition, anytime the printer/MFP is connected using the wireless LAN and a wired LAN, the printer/MFP will automatically reboot in order to connect to the wired LAN.
		Apply Cancel Restore Defaults

ProCurve Switches and Identity Driven Management

This whitepaper has covered the configuration of 802.1X using an HP Jetdirect, and HP ProCurve 6108 switch, and Microsoft's IAS. There are other tools that can supplement this configuration and make it much easier on the Administrator. Three of these tools are: ProCurve Manager, IDM Server, and IDM Agent. IDM stands for Identity Driven Management and is an initiative by HP ProCurve to allow the network to dynamically change its configuration based upon the authentication of the user. A screen shot of IDM is shown in Figure 35 – IDM.

One of the great benefits of this approach is that it allows the administrator to dynamically assign a "networking infrastructure configuration" for the user. Some examples include: VLANs, QoS parameters, network resource restrictions, etc... The wonderful part of this approach is that printing and imaging devices can be integrated into an overall security strategy. Building on the techniques described here, IDM allows printing and imaging devices to be assigned dynamically their own VLAN and QoS parameters as well as restrictions on which resources they can access. It is incredibly powerful.

Identity Management Configuration						×
- Carlos Profiles	Serinting	y and Ima	ging Devices			
Printing and Imaging Devices	Name:	Printing and	I Imaging Devices			
Times	Description:	Printing and	Imaging Devices			
🔤 🗀 Network Resources	Access Att	ributes —				
	VLAN	PID[2]	-	🗖 Don't override		
	QoS:	Normal	-	🗖 Don't override		
	Bandwidth:		1,000,000	🗖 Don't override		
	Network Re	esource Ac	cess Rules ——			
	Action		Resource	Accounting		Edit
					⊆lose	<u>H</u> elp

Figure 35 – IDM

Summary

HP believes 802.1X is a cornerstone of a powerful security strategy. Using the HP ProCurve initiative of Identity Driven Management, powerful security techniques can be utilized by the administrator to protect their Printing and Imaging assets. While Identity Driven Management techniques are powerful, they are not required. Using bundled software such as IAS and any switch that supports RADIUS and 802.1X port-based authentication, we can use HP Jetdirect to participate in almost any customer 802.1X environment.

Appendix A: Troubleshooting 802.1X

Starting with V.38.05 and later firmware, HP Jetdirect has a new capability to log 802.1X information to the Security Page. In the control panel menu for Jetdirect, which starts as "Embedded Jetdirect" or "EIO Jetdirect", enter the menu structure and then go to "Information", then "Print Security Page". A security page will be printed similar to the ones shown in this section. If your HP Jetdirect firmware doesn't support the 802.1X logging or is installed in a Digital Sender only product, we'll need to get a network trace to troubleshoot. Network switches that support 802.1X are fairly sophisticated and they often support the ability to "mirror" a port for network tracing.

We are going to go through a series of 802.1X conditions and show both the 802.1X log and the network trace, which has been filtered to look for only "EAP" packets.

EAP-TLS Success

We need to see what a successful 802.1X session looks like first. Here is the 802.1X log:

Admin Password:	Not Specified	192.168.128.192	
SNMP Versions:	1:2	fe80::21b:78ff:fe	e6:4f40
SNMP Set Cmty Name:	Not Specified	2001:db8:128:0:21	b:78ff:fee6:4f40
SNMP Get Cmty Name:	Not Specified		
Access List:	Not Specified		
Secure Web:	HTTPS Required		
ID Certifi	cate		
ID Certificate:	INSTALLED		
ISSUER CN:	R2	CA C	ertificate
Subject CN:wireless.rem	note.example.inter	CA Certificate:	INSTALLED
Valid From: 200	08-05-06 21:57 UTC	ISSUER CN:	RootCA
Valid To: 200	9-06-29 22:34 UTC	Subject CN:	RootCA
Signature Algorithm:	SHA1	Valid From:	2007-01-06 21:15 UTC
Extended Key Usage:	Not Applicable	Valid To:	2012-01-06 21:22 UTC
Thumbprint:		Signature Algorit	hm: SHA1
SHA1:043fde6ae651599ba5	43bd9999bea9fac84	Extended Key Usaq	e: Not Applicable
MD5: £23554924036ed5	249f3202e7255f56a	Thumbprint:	
		SHA1:f2e99d8c87b9	eacd3e6700c38681c3d0b59
		MD5: ed39e69e0	6491b289a94e96f5542f1af
802.1X Infor	mation		
EAP Method:	TLS		
Encryption Strength:	LOW		
Server ID:	example.internal		
User Name: wireless	@example.internal		
Password:	Not Specified		
Require Exact Match:	Not Set		
Reauthenticate on apply	v: Not Set		
		Error Log	
EAPOL-Start sent			
EAP-Identity request re	ceived		
EAP-Identity 'wireless	example.internal' sent		
Start TLS server auther	tication		
TLS server authenticati	on finished successful	ly	
Start TLS client auther	tication		
TLS client authenticati	on finished successful	ly	

At the bottom of the page we can see the log that shows the activity of the 802.1X supplicant on Jetdirect. However, this security page provides a great snapshot of the configuration of HP Jetdirect for 802.1X and Certificates.

Next, we can see what a network trace looks like for an EAP-TLS success.

© hpprinter.pcap - Ethereal	
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics <u>H</u> elp	
$\blacksquare \blacksquare \blacksquare \blacksquare \blacksquare \models \blacksquare \times @ = \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$	3 💥 🔯
Eilter: Expression Clear Apply	
No Time Source Destination rotoco Info	
<pre>1 0.000000 00:18:fe:84:97:40 Spanning-tree-(for EAP 2 0.000544 HewletP_75:f3:37 Spanning-tree-(for EAP 4 0.419382 HewletP_75:f3:37 Spanning-tree-(for EAP 4 0.419382 HewletP_75:f3:37 Spanning-tree-(for EAP 6 0.464984 HewletP_75:f3:37 Spanning-tree-(for EAP 8 0.510486 HewletP_75:f3:37 Spanning-tree-(for EAP 8 0.510486 HewletP_75:f3:37 Spanning-tree-(for EAP 8 0.510486 HewletP_75:f3:37 Spanning-tree-(for EAP 8 0.510486 HewletP_75:f3:37 Spanning-tree-(for EAP 9 0.511665 00:18:fe:84:97:40 Spanning-tree-(for EAP 9 0.511665 00:18:fe:84:97:40 Spanning-tree-(for EAP 10 0.555736 HewletP_75:f3:37 Spanning-tree-(for EAP 11 0.556877 00:18:fe:84:97:40 Spanning-tree-(for EAP 12 0.693492 HewletP_75:f3:37 Spanning-tree-(for EAP 13 0.694382 00:18:fe:84:97:40 Spanning-tree-(for EAP 14 0.737058 HewletP_75:f3:37 Spanning-tree-(for EAP 15 0.743731 00:18:fe:84:97:40 Spanning-tree-(for EAP 16 0.786068 HewlettP_75:f3:37 Spanning-tree-(for EAP 17 0.793212 00:18:fe:84:97:40 (00:18:fe:84:97:40), Dst: Spanning-tree-(for-bridges)_03 (01:80:c2:00:00:0 18 822.1X Authentication 17 0.793212 00:18:fe:84:97:40 (00:18:fe:84:97:40), Dst: Spanning-tree-(for-bridges)_03 (01:80:c2:00:00:0 18 822.1X Authentication 17 0.79321 0:18:fe:84:97:40 Spanning-tree-(for EAP 18 Extensible Authentication Protocol 18 Extensible Authentication Protocol 16 Code Beauset (1) 17 0 0:18 fe:84:97:40 Spanning-tree-(for EAP 19 Extensible Authentication Protocol 16 Code Beauset (1) 17 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0</pre>	Server Hello rify, Change
Id: 1 Length: 15 Type: Identity [RFC3748] (1) Identity (10 bytes): User name:	
00000 01 80 c2 00 03 00 18 fe 84 97 40 88 8e 01 00	
P: 1/ D: 1/ M: 0	///

Some important packets to look at:

- Packet 1 start of the EAP process, requested by the Authenticator (switch).
- Packet 3 start of the EAP-TLS process
- Packet 4 Jetdirect sends it SSL/TLS Client Hello
- Packet 11 Packets 5, 7, 9, 11 are actually fragmented packets that comprise the Server Hello packet. Packet 11 is what it will look like when it is fully assembled. It is fragmented in this way because the server is sending back certificates which are about 3k octets each in length.
- Packet 14 EAP-TLS requires the client (Jetdirect) to send back a client certificate that is this
 packet.
- Packet 17 the Authenticator indicates "Success" to Jetdirect and EAP-TLS has been negotiated successfully.

Now we know what a good trace is supposed to look like!

EAP Unknown User Name

Let's look at a common failure, which is when the username that HP Jetdirect is sending is unknown by the Authentication Server. Although we are using EAP-TLS, this information is also valid for PEAP.

General Inform	nation	Local I	P Addresses
Admin Password:	Not Specified	192.168.128.192	
SNMP Versions:	1;2	fe80::21b:78ff:fee	5:4£40
SNMP Set Cmty Name:	Not Specified	2001:db8:128:0:21b	:78ff:fee6:4f40
SNMP Get Cmty Name:	Not Specified		
Access List:	Not Specified		
Secure Web:	HTTPS Required		
ID Certific	ate		
ID Certificate:	INSTALLED		
ISSUER CN:	R2	CA Ce	rtificate
Subject CN:wireless.remo	te.example.inter	CA Certificate:	INSTALLED
Valid From: 2008	-05-06 21:57 UTC	ISSUER CN:	RootCA
Valid To: 2009	-06-29 22:34 UTC	Subject CN:	RootCA
Signature Algorithm:	SHA1	Valid From:	2007-01-06 21:15 UTC
Extended Key Usage:	Not Applicable	Valid To:	2012-01-06 21:22 UTC
Thumbprint:		Signature Algorithm	n: SHA1
SHA1:043fde6ae651599ba54	3bd9999bea9fac84	Extended Key Usage	Not Applicable
MD5: f23554924036ed52	49f3202e7255f56a	Thumbprint:	
		SHA1:f2e99d8c87b9ea	acd3e6700c38681c3d0b59
		MD5: ed39e69e064	191b289a94e96f5542f1af
802.1X Inform	ation		
EAP Method:	TLS		
Encryption Strength:	LOW		
Server ID:	example.internal		
User Name: wireles@	example.internal		
Password:	Not Specified		
Require Exact Match:	Not Set		
Reauthenticate on apply:	Not Set		

Here, a simple mistake was made in the name: "wireles" was used instead of "wireless". Here is what a network trace would look like.

🔼 1x-6.pcap - Wireshark	
Elter: Expression Glear Apply	
No Time Source Destination Protocol Info	<u>~</u>
6 29.661779 HewlettP_84:97:40 Spanning-tree-(for EAP Request, Identity [RFG3748] 7 29.662286 HewlettP 75:13:37 Spanning-tree-(for EAP Response, Identity [RFG3748]	
8 30.642660 HewlettP_84:97:40 Spanning-tree-(for EAP Failure	- IB
⊞ Frame 8 (60 bytes on wire, 60 bytes captured)	
8 802.1X Authentication	
version: 1	
Length: 4	
Extensible Authentication Protocol	
code: Fallure (4) Id: 12	
Length: 4	
0000 01 80 C2 00 00 03 00 18 fe 84 97 40 88 8e 01 00	
normal antipation and particular particular information and particular info	
File: "G:\1x+6.pcap" 632 Bytes 00 P: 8 D: 8 M: 0	

Here we see that an EAP request for identity is made via the Authenticator (packet 6). Jetdirect returns a response (packet 7) and then the Authenticator returns an EAP failure (packet 8). The first thing to check in this failure mode is the 802.1X User Name on Jetdirect. The Authentication Server does not recognize the user name that Jetdirect is sending back.

That one was easy.

Server Authentication Problem

Once the EAP identity has been verified, the next step for both EAP-TLS and PEAP is to verify that the authentication server is valid. This validation is done through checking the Server Certificate. Two fields are vitally important in Jetdirect's configuration: The server ID field in the 802.1X configuration and the CA Certificate installed on Jetdirect.

Admin Password: Not Specified SNMP Versions: 1;2 SNMP Set Cmty Name: Not Specified SNMP Get Cmty Name: Not Specified SNMP Get Cmty Name: Not Specified SCURE Web: HTTPS Required 				20200300000000000
Admin Password: Not Specified 192.168.128.192 SNMP Set Cnty Name: Not Specified Access List: Not Specified Access List: Not Specified Access List: Not Specified Access List: Not Specified ID Certificate	General Inform	Nation	Local IP A	ldresses
SAMP Versions: 1,2 SAMP Set Cmty Name: Not Specified SACess List: Not Specified Access List: Not Specified Secure Web: HTTPS Required 	Admin Password:	Not Specified	192.168.128.192	
SAMP Set Cinty Name: Not Specified Access List: Not Specified Secure Web: HTTPS Required 	SNMP Versions:	1;2		
SNMP Get CHCy Name: Not Specified Access List: Not Specified Secure Web: HTTPS Required	SNMP Set Chty Name:	Not Specified		
Access List: Not Specified Secure Web: HTTPS Required ID Certificate: INSTALLED ISSUBE CN: R2 Subject CN: wireless.remote.example.inter Valid From: 2008-05-06 21:57 UTC Subject CN: 2007-01-06 21:15 UTC Subject CN: 2007-01-06 21:15 UTC Extended Key Usage: Not Applicable Valid To: 2017-01-06 21:15 UTC Signature Algorithm: SHA1 Valid From: 2007-01-06 21:15 UTC Extended Key Usage: Not Applicable Valid To: 2012-01-06 21:22 UTC Signature Algorithm: SHA1 Valid From: 2007-01-06 21:15 UTC Extended Key Usage: Not Applicable Valid To: 2012-01-06 21:22 UTC Signature Algorithm: SHA1 SHA1:043fde6ae651599ba543bd999bea9fac84 Extended Key Usage: Not Applicable Thumbprint: SHA1:f2e99ddc87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542flaf Extended Key Usage: Not Applicable Thumbprint: EAP Method: TLS Encryption Strength: LOW Server ID: example.internal Jear Name: wireless@example.internal Password: Not Specified Require Exact Match: Not Set 	SNMP GEC CITCY Name:	Not specified		
Secure web: HTTPS Required	Access List:	Not Specified		
ID Certificate: INSTALLED ID Certificate: INSTALLED ISSUER CN: R2 Subject CN:wireless.remote.example.inter Valid From: 2008-05-06 21:57 UTC ISSUER CN: RootC/ Signature Algorithm: SHAI Valid From: 2007-01-06 21:15 UTC Extended Key Usage: Not Applicable Valid To: 2012-01-06 21:22 UTC Signature Algorithm: SHAI Valid From: 2007-01-06 21:12 UTC Signature Algorithm: SHAI Valid From: 2007-01-06 21:22 UTC Signature Algorithm: SHAI Valid From: 2007-01-06 21:22 UTC Signature Algorithm: SHAI SHA1:043fde5ae651599ba543bd9999bea9fac84 MD5: f23554924036ed5249f3202e7255f56a Thumbprint: SHA1:f2e99d8c87b9eacd3e67D0c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542f1af Extended Key Usage: Not Applicable Tumbprint: LOW Server ID: example.internal Jser Name: wireless@example.internal Der wireless@example.internal Assword: Not Specified Require Exact Match: Not Set APPL-Gentity request received SAPOL-Start sent SAPOL-Start sent SAPT ILS erver ID verification failed Jetdirect Server ID (example.internal' sent Start TLS server authentication Tetdirect Server ID (example.internal) does not match certificate subject name (/CN=w2k3-r me.example.internal) Mert sent: certificate unknown SU/TUS bandsbake error [Ub (20) func(144) reason(134)]	secure web:	HITPS Required		
ID Certificate: INSTALLED ISSUER CN: R2 Subject CN:wireless.remote.example.inter Valid From: 2008-05-06 21:57 UTC ISSUER CN: RootCZ Subject CN: 2009-06-29 22:34 UTC Subject CN: RootCZ Signature Algorithm: SHAL Valid From: 2007-01-06 21:51 UTC Extended Key Usage: Not Applicable Valid To: 2012-01-06 21:22 UTC Signature Algorithm: SHAL SHA1:043fde6ae651599ba543bd9999bea9fac84 MD5: f23554924036ed5249f3202e7255f56a Thumbprint: SHA1:043fde6ae651599ba543bd9999bea9fac84 MD5: d39e69e06491b289a94e96f5542flaf FAP Method: TLS Encryption Strength: LOW Server ID: example.internal Dase Name: wireless@example.internal Dase Name: wireless@example.internal Dase Name: Mireless@example.internal Password: Not Specified Require Exact Match: Not Set SAPOL-Start sent SAPOL-Start sent SAPOL-Start sent SAPOL-Start sent SAPOL-Start sent SAPOL-Start sent SAPOL-Start Sent SAPOL-Start ID (example.internal) Sart TLS server ID verification failed Ietdirect Server ID verification failed Ietdirect Server ID (example.internal) SAPOL-Start sent SAPOL-Start sent	ID Certific	ate		
ISSUER CN: R2 Subject CN:wireless.remote.example.inter Subject CN:wireless.remote.example.inter Subject CN:wireless.remote.example.inter Subject CN: 2009-06-29 22:34 UTC Subject CN: RootCZ Subject CN: RootCZ Subject CN: RootCZ Subject CN: 2007-01-06 21:25 UTC Subject CN: 2007-01-06 21:25 UTC Signature Algorithm: SHAI Valid From: 2007-01-06 21:22 UTC Signature Algorithm: SHAI SHA1:043fde6ae651599ba543bd9999bea9fac84 SHA1:043fde6ae651599ba543bd9999bea9fac84 SHA1:043fde6ae651599ba543bd9999bea9fac84 SHA1:043fde6ae651599ba543bd9999bea9fac84 SHA1:043fde6ae651599ba543bd9999bea9fac84 SHA1:162e99d8c87b9eacd3e6700c3868lc3d0b55 MD5: ed39e69e06491b289a94e96f5542flaf Thumbprint: SHA1:f2e99d8c87b9eacd3e6700c3868lc3d0b55 MD5: ed39e69e06491b289a94e96f5542flaf Server ID: example.internal Jser Name: wireless@example.internal Jser Name: wireless@example.internal Sasword: Not Specified Require Exact Match: Not Set SAP-Identity request received SAP-Identity internal) does not match certificate subject name (/CN=w2k3-r e.example.internal) Nert Sent certificate unknown SL/TLS bandshake error [lib(20) func(144) reason(134)]	ID Certificate:	INSTALLED		
Subject CN:wireless.remote.example.inter CA Certificate: INSTALLER Valid From: 2008-05-06 21:57 UTC ISSUER CN: RootC7 Signature Algorithm: SHAI Valid From: 2007-01-06 21:15 UTC Extended Key Usage: Not Applicable Valid To: 2012-01-06 21:22 UTC Signature Algorithm: SHAI Valid From: 2007-01-06 21:22 UTC Signature Algorithm: SHAI Valid To: 2012-01-06 21:22 UTC Signature Algorithm: SHAI Signature Algorithm: SHAI SHA1:043fde6ae651599ba543bd9999bea9fac84 Extended Key Usage: Not Applicable MD5: f23554924036ed5249f3202e7255f56a Thumbprint: SHA1:f2e99d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542f1af Server ID: example.internal Jser Name: wireless@example.internal Jser Name: wireless@example.internal Password: Not Specified Require Exact Match: Not Set Reauthenticate on apply: Not Set SAPOL-Start sent SAP-Identity request received TAP-Identity request received TAP-Identity request received TAP-Identity request metication Tetdirect server ID (example.internal) does not match certificate subject name (/CN=w2k3-r e.example.internal) Vert sent: certificate unknown SU/TLS bandshake error [lib(20) func(144) reason(134)]	ISSUER CN:	R2	CA Certi:	icate
Valid From: 2008-05-06 21:57 UTC ISSUER CN: RootC2 Valid To: 2009-06-29 22:34 UTC Subject CN: RootC2 Signature Algorithm: SHAL Valid From: 2007-01-06 21:15 UTC Extended Key Usage: Not Applicable Valid To: 2012-01-06 21:22 UTC Thumbprint: Signature Algorithm: SHAI Signature Algorithm: SHAI Extended Key Usage: Not Applicable Valid To: 2012-01-06 21:22 UTC Signature Algorithm: SHAI Signature Algorithm: SHAI SHAI:f2e99d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542f1af SHAI:f2e99d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542f1af SHAI:f2e99d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542f1af SHAI:f2e99d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542f1af SHAI:f2e99d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542f1af SHAI:f2e99d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542f1af SHAI:f2e99d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542f1af SHAI:f2e99d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542f1af SHAI:f2e99d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542f1af SHAI:f2e99d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542f1af SHAI:f2e99d8c87b9eacd3e6700c38681c3d0b55 SHAI:f2e9d8c87b9eacd3e6700c38681c3d0b55 SHAI:f2e9d8c87b9eacd3e6700c38681c3d0b55 SHAI:f2e9d8c87b9eacd3e6700c38681c3d0b55 SHAI:f2e9d8c87b9eacd3e6700c38681c3d0b55 SHAI:f2e9d8c87b9eacd3e6	Subject CN:wireless.remo	te.example.inter	CA Certificate:	INSTALLED
Valid To:2009-06-2922:34 UTCSubject CN:RootCASignature Algorithm:SHAIValid From:2007-01-0621:15 UTCStranded Key Usage:Not ApplicableValid To:2012-01-0621:22 UTCThumbprint:Signature Algorithm:SHAIStA1:043fde6ae651599ba543bd9999bea9fac84Extended Key Usage:Not ApplicableMD5:f23554924036ed5249f3202e7255f56aThumbprint:SHAI:SEAPMD5:ed39e69e06491b289a94e96f5542f1afServer ID:example.internalDser Name:wireless@example.internalDser Name:wireless@example.internalPAPUL-Start sentS02.1X Error LogEAPOL-Start sentServer ID verification failedFar TLS server authenticationfailedBatr TLS server ID verification failedJees not match certificate subject name (/CN=w2k3-rShart TLS server ID verification failedServer ID verification failedJetdirect server ID (example.internal)does not match certificate subject name (/CN=w2k3-rShart TLS server authenticationServer ID verification failedJetdirect server ID (example.internal)does not match certificate subject name (/CN=w2k3-rSe.example.internal)loes not match certificate subject name (/CN=w2k3-rSu/TLS bandshake error[13(2)]Su/TLS bandshake error[13(2)]Su/TLS bandshake error[13(2)]	Valid From: 2008	-05-06 21:57 UTC	ISSUER CN:	RootCA
Signature Algorithm: SHAI Valid From: 2007-01-06 21:15 UTC Extended Key Usage: Not Applicable Valid To: 2012-01-06 21:22 UTC Thumbprint: Signature Algorithm: SHAI Signature Algorithm: ShAI ShAI:f2e99d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542f1af ShAI:f2e99d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542f1af ShAI:f2e99d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542f1af ShAI:f2e99d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542f1af ShAI:f2e99d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542f1af ShAI:f2e99d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542f1af ShAI:f2e99d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542f1af ShAI:f2e9d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542f1af ShAI:f2e9d8c87b9eacd3e67b9ea	Valid To: 2009	-06-29 22:34 UTC	Subject CN:	RootCA
Extended Key Usage: Not Applicable Valid To: 2012-01-06 21:22 UTC Thumbprint: SHA1:043fde6ae651599ba543bd9999bea9fac84 Extended Key Usage: Not Applicable MD5: f23554924036ed5249f3202e7255f56a Thumbprint: SHA1:f2e99d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542f1af EAP Method: TLS Encryption Strength: LOW Server ID: example.internal Dassword: Not Specified Require Exact Match: Not Set EAPOL-Start sent EAP-Identity request received EAP-Identity FAP-Identity for the	Signature Algorithm:	SHA1	Valid From: 20	07-01-06 21:15 UTC
Thumbprint: SHAI Signature Algorithm: SHAI SHA1:043fde6ae651599ba543bd9999bea9fac84 Extended Key Usage: Not Applicable Thumbprint: SHAI SHA1:f2e99d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542flaf SHA1:f2e99d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542flaf SHAI:f2e99d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542flaf SHAI:f2e99d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542flaf SHAI:f2e99d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542flaf SHAI:f2e99d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542flaf SHAI:f2e9d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542flaf SHAI:f2e9d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542flaf SHAI:f2e9d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542flaf SHAI:f2e9d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542flaf SHAI:f2e9d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542flaf SHAI:f2e9d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542flaf SHAI:f2e9d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542flaf SHAI:f2e9d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542flaf SHAI:f2e9d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542flaf SHAI:f2e9d8c87b9eacd3e6700c38681c3d0b55 SHAI:f2e9d8c87b9eacd3e67b9ea	Extended Key Usage:	Not Applicable	Valid To: 20	12-01-06 21:22 UTC
SHA1:043fde6ae651599ba543bd9999bea9fac84 MD5: f23554924036ed5249f3202e7255f56a MD5: f23554924036ed5249f3202e7255f56a SHA1:f2e99d8c87b9eacd3e6700c38681c3d0b59 MD5: ed39e69e06491b289a94e96f5542f1af MD5: ed39e69e06491b289a94e96f5542f1af Server ID: Example.internal User Name: wireless@example.internal Desrver ID: example.internal Desrver ID: Not Specified Require Exact Match: Not Set Reauthenticate on apply: Not Set SAPOL-Start sent SAPOL-Start sent SAPOL-Start sent SAPOL-Start request received SAP-Identity 'wireless@example.internal' sent Start TLS server authentication Jetdirect server ID (example.internal) does not match certificate subject name (/CN=w2k3-r me.example.internal) Ner sent: certificate unknown SSL/TLS bandshake error []ib(20) func(144) reason(134)]	Thumbprint:	**	Signature Algorithm:	SHA1
MD5: f23554924036ed5249f3202e7255f56a Thumbprint: SHA1:f2e99d8c87b9eacd3e6700c38681c3d0b55 MD5: ed39e69e06491b289a94e96f5542f1af MD5: ed39e06491b289a94e96f5542f1af MD5:	SHA1:043fde6ae651599ba54	3bd9999bea9fac84	Extended Key Usage:	Not Applicable
SHA1:f2e99d&c87b9eacd3e6700c38681c3d0b59 MD5: ed39e69e06491b289a94e96f5542f1af EAP Method: TLS Encryption Strength: LOW Server ID: example.internal Der Name: wireless@example.internal Password: Not Specified Require Exact Match: Not Set Reauthenticate on apply: Not Set 	MD5: f23554924036ed52	49f3202e7255f56a	Thumborint:	
MD5: ed39e69e06491b289a94e96f5542f1af MD5: ed39e69e06491b289a94e96f5542f1af EAP Method: TLS Encryption Strength: LOW Server ID: example.internal Jser Name: wireless@example.internal Password: Not Specified Require Exact Match: Not Set Reauthenticate on apply: Not Set EAPOL-Start sent EAP-Identity request received EAP-Identity 'wireless@example.internal' sent Start TLS server authentication Tetdirect Server ID verification failed Tetdirect server ID (example.internal) does not match certificate subject name (/CN=w2k3-r me.example.internal) Nert sent: certificate unknown SU/TLS bandshake error [lib(20) func(144) reason(134)]			SHA1: f2e99d8c87b9eacd	e6700c38681c3d0b59
EAD Method: TLS EAD Method: TLS Encryption Strength: LOW Server ID: example.internal Deer Name: wireless@example.internal Password: Not Specified Require Exact Match: Not Set Reauthenticate on apply: Not Set 			MD5 · od39e69e06491)	289294096f5542f1af
EAP Method: TLS Encryption Strength: LOW Server ID: example.internal Jser Name: wireless@example.internal Password: Not Specified Require Exact Match: Not Set Reauthenticate on apply: Not Set 	802 1X Inform	ation		205454650155421141
Encryption Strength: LOW Server ID: example.internal Jser Name: wireless@example.internal Password: Not Specified Require Exact Match: Not Set Reauthenticate on apply: Not Set SAPOL-Start sent SAPOL-Start sent SAPOL-Start sent SAP-Identity request received SAP-Identity 'wireless@example.internal' sent Start TLS server authentication fatiled Jetdirect Server ID verification failed Jetdirect server ID (example.internal) does not match certificate subject name (/CN=w2k3-r se.example.internal) Alert sent: certificate unknown SSL/TLS bandshake error []ib(20) func(144) reason(134)]	FAD Method.	TIC		
Server ID: example.internal User Name: wireless@example.internal Password: Not Specified Require Exact Match: Not Set Reauthenticate on apply: Not Set SAPOL-Start sent EAPOL-Start sent EAPOL-Start request received EAP-Identity 'wireless@example.internal' sent Start TLS server authentication Jetdirect Server ID verification failed Jetdirect server ID (example.internal) does not match certificate subject name (/CN=w2k3-r me.example.internal) Nert sent: certificate unknown SSL/TLS handshake error [lib(20) func(144) reason(134)]	Encryption Strength.	LON		
Default Default Der Name: wireless@example.internal Password: Not Specified Require Exact Match: Not Set Reauthenticate on apply: Not Set SAP-Identity request received 802.1X Error Log EAPOL-Start sent SAP-Identity request received EAP-Identity request received Set EAT TLS server authentication Jetdirect Server ID verification failed Jetdirect Server ID (example.internal) does not match certificate subject name (/CN=w2k3-r Se.example.internal) Vlet sent: certificate unknown SSL/TLS handshake error [lib(20) func(144) reason(134)]	Perver ID.	ovample internal		
Set Name: Wireless@example.internal Password: Not Specified Require Exact Match: Not Set Reauthenticate on apply: Not Set EAPOL-Start sent 802.1X Error Log EAP-Identity request received 3AP-Identity 'wireless@example.internal' sent Start TLS server authentication Failed Jetdirect Server ID verification failed Jetdirect server ID (example.internal) does not match certificate subject name (/CN=w2k3-r Sec.ample.internal) Alert sent: certificate unknown SSL/TLS handshake error [][b(20) func(144) reason(134)]	lass Name. wireless	example internal		
Require Exact Match: Not Set Require Exact Match: Not Set SAPOL-Start sent EAP-Identity request received SAP-Identity 'wireless@example.internal' sent Start TLS server authentication Betdirect Server ID verification failed Jetdirect server ID (example.internal) does not match certificate subject name (/CN=w2k3-r me.example.internal) Alert sent: certificate unknown SSL/TLS bandshake error []ib(20) func(144) reason(134)]	Dsei Name: wirelesse	example.internal		
Reauthenticate on apply: Not Set Reauthenticate on apply: Not Set SAP-Identity request received EAP-Identity request received EAP-Identity 'wireless@example.internal' sent Start TLS server authentication Jetdirect Server ID verification failed Jetdirect server ID (example.internal) does not match certificate subject name (/CN=w2k3-r se.example.internal) Alert sent: certificate unknown SSL/TLS bandshake error []ib(20) func(144) reason(134)]	Password:	Not specified		
Reauthenticate on apply: Not Set 	Require Exact Match:	NOT SET		
EAPOL-Start sent EAPOL-Start sent EAP-Identity request received EAP-Identity 'wireless@example.internal' sent Start TLS server authentication Jetdirect Server ID verification failed Jetdirect server ID (example.internal) does not match certificate subject name (/CN=w2k3-r me.example.internal) Alert sent: certificate unknown SSL/TLS handshake error [lib(20) func(144) reason(134)]	Reauthenticate on apply:	Not Set		
EAPOL-Start sent EAP-Identity request received EAP-Identity 'wireless@example.internal' sent Start TLS server authentication Tetdirect Server ID verification failed Jetdirect server ID (example.internal) does not match certificate subject name (/CN=w2k3-r me.example.internal) Alert sent: certificate unknown SU/TLS handshake error [lib(20) func(144) reason(134)]		802.1X 1	Error Log	
EAP-Identity request received EAP-Identity 'wireless@example.internal' sent Start TLS server authentication Jetdirect Server ID verification failed Jetdirect server ID (example.internal) does not match certificate subject name (/CN=w2k3-r me.example.internal) Alert sent: certificate unknown SSL/TLS handshake error [lib(20) func(144) reason(134)]	EAPOL-Start sent			
EAP-Identity 'wireless@example.internal' sent Start TLS server authentication Jetdirect Server ID verification failed Tetdirect server ID (example.internal) does not match certificate subject name (/CN=w2k3-r me.example.internal) Nert sent: certificate unknown SEL/TLS handshake error []ib(20) func(144) reason(134)]	EAP-Identity request rec	eived		
Start TLS server authentication Jetdirect Server ID verification failed Jetdirect server ID (example.internal) does not match certificate subject name (/CN=w2k3-r e.example.internal) Alert sent: certificate unknown SEL/TLS handshake error [lib(20) func(144) reason(134)]	EAP-Identity 'wireless@e	xample.internal' sent		
Jetdirect Server ID verification failed Jetdirect server ID (example.internal) does not match certificate subject name (/CN=w2k3-r æ.example.internal) Alert sent: certificate unknown SSL/TLS handshake error [lib(20) func(144) reason(134)]	Start TLS server authent	ication		
Jetdirect server ID (example.internal) does not match certificate subject name (/CN=w2k3-r ee.example.internal) Alert sent: certificate unknown SSL/TLS handshake error [lib(20) func(144) reason(134)]	Jetdirect Server ID veri	fication failed		
ee.example.internal) Alert sent: certificate unknown SSL/TLS handshake error []ib(20) func(144) reason(134)]	Jetdirect server ID (exa	mple.internal) does no	ot match certificate subject	t name (/CN=w2k3-r
Alert sent: certificate unknown SSL/TLS handshake error []ib(20) func(144) reason(134)]	e.example.internal)			
SL/TLS handshake error $[1ib(20) func(144) reason(134)]$	Alert sent, certificate	unknown		
AND FOR THE PROPERTY AND THE PROPERTY AN	and have be all hand a local to the dealer to the first to the first to the	CARACTER OF WELL		
	SSL/TLS handshake error	[lib(20) func(144) rea	ason(134)]	

Here we can see that the server authentication failed. We see clearly from the log that the server ID field of JD does not match the subject name of the certificate. Let's look at different failure, but still a server authentication issue:

```
HP Jetdirect Security Page (1/4) ( English - PCL )
----- General Information -----
                                                          ----- Local IP Addresses -----
Admin Password: Not Specified
                                                       192.168.128.192
SNMP Set Cmty Name: Not Specified
SNMP Get Cmty Name: Not Specified
Access List: Not Specified
Secure Web:
                            HTTPS Required
   ----- ID Certificate -----
ID Certificate:
                                 INSTALLED
ISSUER CN:
                                                        ----- CA Certificate -----
ISSUER CN:
Subject CN:wireless.remote.example.ince
Valid From: 2008-05-06 21:57 UTC
Valid To: 2009-06-29 22:34 UTC
SHA1
                                          R2
                                                     CA Certificate: INSTALLED
ISSUER CN: RootCA
                                                                                            RootCA
Valid To: Snai
Signature Algorithm: Snai
Not Applicable
                                                        Subject CN:
                                                        Subject CN:
Valid From: 2007-06-29 22:24 UTC
Valid To: 2009-06-29 22:34 UTC
Signature Algorithm: SHA1
                                                                                                   R2
                                                       Valid To: 2009-06-29 22:34 UTC
Signature Algorithm: SHA1
Extended Key Usage: Not Applicable
Thumbprint:
SHA1:043fde6ae651599ba543bd9999bea9fac84
MD5:
        f23554924036ed5249f3202e7255f56a
                                                       Thumbprint:
                                                        SHA1:6d6a18071458a4300ab52d230bfd8547fd5
                                                        MD5: 0b9094dbc0cfdf00142a33de1bfdf259
 ----- 802.1X Information ------
EAP Method:
                                          TLS
EAP Method: TLS
Encryption Strength: LOW
Server ID: example.internal
Server ID:
              wireless@example.internal
User Name:
rassword: Not Specified
Require Exact Match: Not Set
Require Exact Match: Not Set
Reauthenticate on apply: Not Set
                 802.1X Error Log -----
EAPOL-Start sent
EAP-Identity request received
EAP-Identity 'wireless@example.internal' sent
Start TLS server authentication
X509 error: unable to get local issuer certificate
Cert 0: Issuer: /DC=internal/DC=example/CN=RootCA
Cert 0: Subject: /CN=w2k3-r2-ee.example.internal
Cert 0: Expires on: 2008-04-22 22:46 UTC
Cert 0: Signature Algorithm: shalWithRSAEncryption
Alert sent: unknown CA
SSL/TLS handshake error [lib(20) func(144) reason(134)]
EAP-NAK sent
EAP-Failure received
```

Here we can see that we have an "unknown CA" error. In the log, the certificate issuer is RootCA but SSL is complaining that it cannot get the certificate for the local issuer. In other words, the certificate for RootCA is unavailable which points to the wrong CA certificate being installed on Jetdirect.

Let's look at a network trace.



Here are the important packets in this trace:

- Packet 210 Server Hello where the Authentication Server's certificate is sent to Jetdirect.
- Packet 211 Jetdirect sends a NAK.

What has happened here is that Jetdirect does not accept the Authentication Server's certificate and refuses to continue. Things to check:

- The CA certificate configured on Jetdirect. This field must be configured to be a Root CA of the chain in use.
- The 802.1X Server ID field on Jetdirect be sure that it is configured correctly. You may try just to set it to blank until you can get 802.1X up and running.
- Be sure that the certificate being returned by the Authentication Server is the one you believe is being returned. All of these things are easy to check. Let's look at packet 210 in depth.

1 1x-1.pcap - Wireshark	7 🗙
Ele Edit View Go Capture Analyze Statistics Help	1.11.11
Elter: Qear Apply	
No Time Source Destination Protocol Info	^
210 1078.0788: HewlettP_84:97:40 Spanning-tree-(for TLSv1 Server Hello, Certificate, Certificate Request, Server Hello Done 211 1078.1243: HewlettP 75:f3:37 Spanning-tree-(for EAP Response, Legacy Nak (Response only) [RFG3748]	
212 1107.7375; HewlettP 84:97:40 Spanning-tree-(for EAP Failure	
⊕ Frame 210 (1450 bytes on wire, 1450 bytes captured)	~
■ Ethernet II, Src: HewlettP_84:9/:40 (00:18:te:84:9/:40), Dst: Spanning-tree-(tor-bridges)_03 (01:80:c2:00:00:03)	
version: 1	
Type: EAP Packet (0)	
Length: 1432	
B Extensible Authentication Protocol	
Code: Request (1)	
10: 1/5	
Tyme: EAP-TIS [REC7716] [Aboha] (13)	
Flacs(0x0):	
⊞ [EAP-TLS Fragments (5790 bytes): #204(1452), #206(1456), #208(1456), #210(1426)]	
B Secure Socket Layer	
🖻 TLSv1 Record Layer: Handshake Protocol: Multiple Handshake Messages	
Content Type: Handshake (22)	
Version: TLS 1.0 (0x0301)	
Rendsha protocol: Sorver Hallo	
Handshake Type: Certificate (11)	
Length: 2542	
Certificates Length: 2539	
д Certificates (2539 bytes)	
Certificate Length: 1202	
⊞ Certificate: 30820417A003020102020A611A0AEE0000000005300D06 (id-at-commonName=ias.example.internal)	
Certificate Length: 1331	-
B Certificate: 302041/A033220222042/35356-00000000013000001. (Id-at-Commonwame=K2, CCICL 9, 2342, 19200300, 100, 1, 23=example B Handshaka Protocol: Cartificate Paquest	,
	2
0050 00 09 00 00 00 00 00 00 00 00 00 00 00	~
Frame (1450 bytes) Reassembled EAP-TLS (5790 bytes)	
List of certificates (ssl.handshake P: 212 D: 212 M: 0	

Here we can see that there are 2 certificates being returned by the Authentication Server:

- "ias.example.internal" issued by R2, an intermediate certificate authority
- "R2.example.internal" issued by RootCA, the root certificate authority.

The first certificate is the IAS server's certificate that Jetdirect will check the Server ID field against. Therefore, the server ID field needs to be configured correctly based upon the common name of "ias.example.internal". The next certificate is part of the chain that is sent back to the client. This is R2's certificate. Let's look at these more closely.

🛽 1x-1.pcap - Wireshark
Ele Edit View Go Capture Analyze Statistics Help
Elter: Elter: E
No Time Source Destination Protocol Info
210 1078 0788: Hewlettp_B4:97:40 Spanning-tree-(for TLSv1 Server Hello, Certificate, Certificate Request, Server Hello Done
211 10/6.1243 new lettp=/3:13:37 Spanning-tree-(for EAP Response, Legacy Nak (Response only) [RFC3/46]
Certificate: 202041240020201020204611404FE0000000005200006 (id at commonlymetics orympia internal)
B certificate
version: v3 (2)
serialNumber : 0x611a0aee0000000005
☐ issuer: rdnSequence (0)
⊞ rdnSequence: 3 items (id-at-commonName=R2,ccitt.9.2342.19200300.100.1.25=example,ccitt.9.2342.19200300.100.1.25=internal;
walidity
subject. runsequence () k rdssequence: i tiam (id.at.commonName-iac.example internal)
B subject publickey of the common value rate common value rate and the first state of the subject build state of the subject buil
Busices Busices Busices
Padding: 0
encrypted: 896Ac544BA1D67A56A70AF623E555AB7EEE8FF680339A6EB
Certificate Length: 1331
□ Certificate: 30820417A003020102020A1675356F00000000011300D06 (id-at-commonName=R2,ccitt.9.2342.19200300.100.1.25=example,cc
SignedCertificate
version: Vs (2)
Seria number : 0x16/3536100000000011
B rdnsequence: 3 items (id-at-commonName=RootCA.ccitt.9.2342.19200300.100.1.25=example.ccitt.9.2342.19200300.100.1.25=inter
H validity
🗉 subject: rdnSequence (0)
🗄 rdnSequence: 3 items (id-at-commonName=R2,ccitt.9.2342.19200300.100.1.25=example,ccitt.9.2342.19200300.100.1.25=internal)
🗄 subjectPublicKeyInfo
B extensions: 8 items
00e0 32 35 5a 30 1f 31 1d 30 1b 06 03 55 04 03 13 14 2520 10U 00f0 69 61 73 2e 65 78 61 6d 70 6c 65 2e 69 6e 74 65 Tas.exam ple.inte 0100 72 6e 61 6c 30 81 9f 30 0d 06 09 2a 86 48 86 f7 rnal00*H
Frame (1450 byttes) Reassembled EAP-Tr25 (5790 byttes)
x509if.RDNSequence (x509af.rdn] P: 212.D: 212 M: 0

By looking at each certificate's "Issuer" and "Subject" fields, we can determine what is Jetdirect is seeing. Since "ias.example.internal" is the Authentication Server certificate and its common name is shown as "ias.example.internal", we know that the Server ID needs to be configured correctly to handle that value. The "Issuer" of this certificate is R2.example.internal. Jetdirect needs to have the public key certificate of R2 in order to verify the signature on ias.example.internal. The Authentication Server also sends back the R2.example.internal certificate. This certificate is issued by RootCA. Jetdirect also needs the RootCA public key certificate. This certificate, RootCA must be configured on Jetdirect as the CA Certificate in order for the certificate chain to be verified.

These two situations are the most common type of issues that affect 802.1X configurations.

Client Authentication Problem

Assuming that everything went ok with Server Authentication, then client authentication is the next area where there could be problems. For EAP-TLS, the client sends a certificate to authenticate while in PEAP, a username/password is sent using a different protocol to authenticate the client. In both cases, the certificate or the username/password must be mapped to an account that is granted access. Let's look at an EAP-TLS client authentication problem.

HP Jetdirect Sec	urity Page (1/4)	(English - PCL)
General Infor	mation	Local IP	Addresses
Admin Password:	Not Specified	192.168.128.192	
SNMP Versions:	1;2		
SNMP Set Cmty Name:	Not Specified		
SNMP Get Cmty Name:	Not Specified		
Access List:	Not Specified		
Secure Web:	HTTPS Required		
ID Certifi	cate		
ID Certificate:	INSTALLED		
ISSUER CN:	R2	CA Cert	ificate
Subject CN:wireless.rem	ote.example.inter	CA Certificate:	INSTALLED
Valid From: 200	8-05-06 21:57 UTC	ISSUER CN:	RootCA
Valid To: 200	9-06-29 22:34 UTC	Subject CN:	RootCA
Signature Algorithm:	SHA1	Valid From:	2007-01-06 21.15 UTC
Extended Key Usage:	Not Applicable	Valid To:	2012-01-06 21:22 UTC
Thumborint	nee nppiloubic	Signature Algorithm.	2012 01 00 21.22 010
SHA1:043fde6ae651599ba5	43bd9999bea9fac94	Extended You Users.	Not Appliable
MD5 · f23554924036ed5	249f3202o7255f56	Thumbariat	NOL Applicable
100. 120004024000cd0.	24915202872551508		12 5700 20500 2101 50
		SHAL:1209908C8/D9ead	cd3e6700c38681c3d0b59
802 1¥ I=f		MD5: ed39e69e0645	1£289a94e96f5542f1af
END Mathad	mation		
EAP Method:	TLS		
Encryption Strength:	LOW		
Server ID:	example.internal		
User Name: wireless	@example.internal		
Password:	Not Specified		
Require Exact Match:	Not Set		
Reauthenticate on apply	: Not Set		
	802.1X Er	cror Log	
EAPOL-Start sent			
EAP-Failure received			
EAP-Identity request real	ceived		
EAP-Identity 'wireless@e	example.internal' sent		
Start TLS server authent	tication		
TLS server authenticatio	on finished successfully	/	
Start TLS client authent	tication		
Alert received: access of	denied		
SSL/TLS handshake error	[]ib(20) func(148) reas	on (1049) 1	
EAP-NAK sent	((20) Func (140) Teas	ANT (TO 33/]	
EAP-Failure received			
SL/TLS handshake error AP-NAK sent AP-Failure received	[lib(20) func(148) reas	son(1049)]	

Notice that "TLS Server Authentication finished successfully". Based upon that message, we've eliminated a lot of things that could have gone wrong. However, the message "Alert Received: access denied" tells us that the client authentication failed. Let's look at a trace and then we'll talk about some of the things to check.

	Ethereal		
<u>File Edit View C</u>	<u>Go</u> <u>C</u> apture <u>A</u> nalyze	Statistics Help	
	🌒 🗁 🖪 🗙 🤅	≥ 🗳 🗳 ቅ	♥ 7 ½ 🗏 🗟 0, 0, 0, 10 ₩ 14 15 16 10
Eilter: eap		• E	xpression <u>C</u> lear <u>A</u> pply
No. Time 17 15.489268 18 15.489268 18 15.489813 20 15.55216 21 15.55216 22 15.546357 24 15.644133 26 15.644133 27 15.689401 28 15.600549 29 15.826018 29 15.826018 20 15.406876 59 45.008276 54 500549 20 15.826018 21 15.412380 64 45.127010 63 45.1278380 64 45.1278380 63 45.174856 64 45.174866	Source 00:18:fe:84:97:40 Hewl ettp-75:f3:37 00:18:fe:84:97:40 Hewl ettp-75:f3:37 00:18:fe:84:97:40 Howl ettp-75:f3:37 00:18:fe:84:97:40 Howl ettp-75:f3:37 00:18:fe:84:97:40 Hewl ettp-75:f3:37 00:18:fe:84:97:40 Hewl ettp-75:f3:37 00:18:fe:84:97:40 Hewl ettp-75:f3:37 00:18:fe:84:97:40 Hewl ettp-75:f3:37 Hewl ettp-75:f3:37 00:18:fe:84:97:40 Hewl ettp-75:f3:37 Hewl ettp	Destination nr Spanning-tree-(for E spanning-tree-(for E spanning-tree-(for T spanning-tree-(for T spanning-tree-(for T spanning-tree-(for T spanning-tree-(for T spanning-tree-(for T spanning-tree-(for T spanning-tree-(for T spanning-tree-(for T spanning-tree-(for E spanning-tree-(for E spanning-tree-(for E spanning-tree-(for E spanning-tree-(for E spanning-tree-(for T spanning-tree-(for T spanning-tree-(for T spanning-tree-(for E spanning-tree-(for E spanning-tree-(for E spanning-tree-(for E spanning-tree-(for E spanning-tree-(for E spanning-tree-(for E spanning-tree-(for E spanning-tree-(for E	Date Info AP Request, Identity [RFC3748] Response, Identity [RFC3748] AP Response, Identity [RFC3748] AP Request, EAP-TLS [RFC2716] [Aboba] Client Hello Server Hello, Certificate, Certificate Request, Server Hello Done Response, EAP-TLS [RFC2716] [Aboba] Server Hello, Certificate, Certificate Request, Server Hello Done Response, EAP-TLS [RFC2716] [Aboba] Server Hello, Certificate, Certificate Request, Server Hello Done Response, EAP-TLS [RFC2716] [Aboba] Server Hello, Certificate, Certificate Request, Server Hello Done Response, Identity [RFC3748] Request, Identity [RFC3748] Request, LAP-TLS [RFC2716] [Aboba] Client Hello LS Server Hello, Certificate, Certificate Request, Server Hello Done Server Hello, Certificate, Certificate, Request, Server Hello Done Server Hello, Certificate, Certificate Request, Server Hello Done Response, EAP-TLS [RFC2716] [Aboba] Server Hello, Certificate, Certificate Request, Server Hello Done
65 45.218006 66 45.219148 67 45.263194 68 45.264370 69 45.399427 70 45.411675 71 45.434233	HewlettP_75:f3:37 00:18:fe:84:97:40 HewlettP_75:f3:37 00:18:fe:84:97:40 HewlettP_75:f3:37 00:18:fe:84:97:40 HewlettP_75:f3:37	Spanning-tree-(for E Spanning-tree-(for T Spanning-tree-(for T Spanning-tree-(for T Spanning-tree-(for T Spanning-tree-(for E	AP Response, EAP-TLS [RFC2716] [Aboba] LS Server Hello, Certificate, Certificate Request, Server Hello Done AP Response, EAP-TLS [RFC2716] [Aboba] LS Server Hello, Certificate, Certificate Request, Server Hello Done LS Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Client Hello[Malformed Packet] LS Alert (Level: Fatal, Description: Access Dented) AP Response, Nak (Response only) [RFC3748]
■ Ethernet II, Sri 802.1X Authenti Version: 1 Type: EAP Pack Length: 17 ■ Extensible Aut Code: Reques Id: 18 Length: 17 Type: EAP-TI Flag(Ox80): Length: 7 ■ Secure Socke ■ TLS Recore Content	c: 00:18:fe:84:97:4C cation (et (0) thentication Protoco t (1) .s [RFC2716] [Aboba] Length et Layer Layer: Alert (Leve Yupe: Alert (21)	(00:18:fe:84:97:40), 1 (13) 1: Fatal, Description	Dst: spanning-tree-(for-bridges)_03 (01:80:c2:00:00:03) : Access Denied)
Version: Length: ⊞ Alert Me	TLS 1.0 (0x0301) 2 ssage		

Here we can see that the Server Hello was sent (packet 68) and it must have been accepted because Jetdirect sends the client certificate (packet 69) and did not send a NAK. However, after the client certificate is sent, the Authenticator returns a TLS Alert indicating "Access Denied". There are a few of things to check:

- The Jetdirect Identity Certificate must be configured
- The Jetdirect Identity Certificate must be one the Authentication Server Trusts
- The Jetdirect user in Active Directory must have Jetdirect's certificate mapped to the account that represents Jetdirect.

PEAP

Almost everything we've covered with EAP-TLS is also valid for PEAP. Let's look at a successful PEAP negotiation.



Admin Password: SNMP Versions: SNMP Set Cmty Na SNMP Get Cmty Na	l Information	Specified 1;2 Specified Specified	Local IP Addr 192.168.128.192 fe80::21b:78ff:fee6:4f40 2001:db8:128:0:21b:78ff:	resses) fee6:4f40
Access List: Secure Web:	Not S HTTPS	Specified Required		
ID	Certificate			
ID Certificate:	1	INSTALLED		
ISSUER CN:		R2	CA Certific	ate
Subject CN:wirel	ess.remote.examp	ple.inter	CA Certificate:	INSTALLED
Valid From:	2008-05-06 2	21:57 UTC	ISSUER CN:	RootCA
Valid To:	2009-06-29 2	22:34 UTC	Subject CN:	RootCA
Signature Algori	thm:	SHA1	Valid From: 2007	-01-06 21:15 UTC
Extended Key Usa	ge: Not Ap	pplicable	Valid To: 2012	-01-06 21:22 UTC
Thumbprint:			Signature Algorithm:	SHA1
SHA1:043fde6ae65	1599ba543bd9999b	bea9fac84	Extended Key Usage:	Not Applicable
MD5: f2355492	4036ed5249f3202€	e7255f56a	Thumbprint:	
			SHA1:f2e99d8c87b9eacd3e6	700c38681c3d0b59
			MD5: ed39e69e06491b28	9a94e96f5542flaf
802.1	X Information			
EAP Method:	224 8 41 0	PEAP		
Encryption Streng	gth:	LOW		
Server ID:	example.	internal		
User Name: w:	ireless@example.	internal		
Password:	5	Specified		
Require Exact Mat	tch:	Not Set		

Here is the log output from a successful PEAP negotiation. An important thing to notice is the EAP-MSCHAPv2 client authentication method. There are a variety of ways that are used to send the username/password to the authentication server, this is one of them.

I tx-2.pcap - Wireshark
jle Edit Vjew Go Capture Analyze Statistics Help
≝≝≝≝≥™≥™×∿≞]q+⇒∞7₽] ⊒ qqqq"≝⊠±%
jiter: eap 💌 Expression Qear Apply
Io Time Source Destination Protocol Info
Bill Decknam Paduca Decknam 1 0.00000 HewlettP_84:97:40 Spanning-tree-(for EAP Request, Identity [RFC3748] 2 0.000567 HewlettP_75:f3:37 Spanning-tree-(for EAP Request, Identity [RFC3748] 4 0.130857 HewlettP_75:f3:37 Spanning-tree-(for EAP Request, EAP-TLS [RFC3748] 5 0.142255 HewlettP_75:f3:37 Spanning-tree-(for EAP Request, PEAP [Palekar] 6 0.193462 HewlettP_75:f3:37 Spanning-tree-(for EAP Request, PEAP [Palekar] 7 0.299056 HewlettP_75:f3:37 Spanning-tree-(for EAP Request, PEAP [Palekar] 8 0.343181 HewlettP_75:f3:37 Spanning-tree-(for EAP Response, PEAP [Palekar] 10 0.388759 HewlettP_75:f3:37 Spanning-tree-(for EAP Response, PEAP [Palekar] 12 0.433831 HewlettP_75:f3:37 Spanning-tree-(for TLSV Server Hello, Certificate, Crificate Request, Server Hello Done 14 0.23037 HewlettP_81:97:40 Spanning-tree-(for TLSV Server Hello, Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
Frame 25 (60 bytes on wire, 60 bytes captured)
BUILTS AUTHENTICE 11, STC: NEWTELT_G4:9/:40 (00:18:TE:84:9/:40), DST: Spanning-Tree-(Tor-Dridges)_03 (01:80:C2:00:00:03) 802.1X Authentication
Version: 1 Type: EAP Packet (0) Length: 4
Extensible Authentication Protocol Code: Success (3) Id: 13 Length: 4
000 01 80 c2 00 03 00 18 fe 84 97 40 88 8e 01 00
le: "C:\Documents and Settings P: 25 D: 25 M: 0

Packets 17-24 are where the User Name / Password are sent over and verified. Packet 25 shows an EAP Success, which indicates that everything went fine. Note that in packet 14, it appears that the client certificate is sent over, but it is not. When using EAP-TLS, it is sent, but when using PEAP, the TLS connection is established without sending over the client certificate.

There is one case where a wrong password can be configured on Jetdirect and get a failure.

HP Jetdirect Sec	urity Page (1/4)	(English - PCL)
General Infor Admin Password: SNMP Versions: SNMP Set Cmty Name: SNMP Get Cmty Name: Access List: Secure Web:	Not Specified 1;2 Not Specified Not Specified Not Specified HTTPS Required	Local IP Addresses 192.168.128.192 fe80::21b:78ff:fee6:4f40 2001:db8:128:0:21b:78ff:fee6:4f40
ID Certifi	cate	
ID Certificate: ISSUER CN: Subject CN:wireless.rem Valid From: 200 Valid To: 200 Signature Algorithm: Extended Key Usage: Thumbprint: SHA1:043fde6ae651599ba5 MD5: f23554924036ed5	INSTALLED R2 R2 R0te.example.inter 8-05-06 21:57 UTC 9-06-29 22:34 UTC SHA1 Not Applicable 43bd9999bea9fac84 249f3202e7255f56a	CA Certificate CA Certificate: INSTALLED ISSUER CN: RootCA Subject CN: RootCA Valid From: 2007-01-06 21:15 UTC Valid To: 2012-01-06 21:22 UTC Signature Algorithm: SHA1 Extended Key Usage: Not Applicable Thumbprint: SHA1:f2e99dc&7b9eacd3e6700c38681c3d0559
802.1X Infor	mation	MD5: ed39e69e06491b289a94e961554211a1
EAP Method: Encryption Strength: Server ID: User Name: wireless Password: Require Exact Match: Reauthenticate on apply	PEAP LOW example.internal Specified Not Set : Not Set	
EAP-Identity request re EAP-Identity 'wireless® Start PEAP server auther PEAP server authenticat Start EAP-MSCHAPv2 clie Invalid password, check EAP-MSCHAPv2 client aut	ceived example.internal' sent ntication ion finished successfull nt authentication the password entered or hentication failed	rror Log ly n Jetdirect

The log shows password errors in PEAP very clearly! The network trace isn't as clear.

🥙 (Untitled) - Ethereal	
Eile Edit View Go Capture Analyze Statistics Help	
	* 🗢 🛧 生 🗐 🖳 🔍 🔍 🔍 🗠 🎬 🖉 🔛 💥 🔯
Eilter: eap 🗾 💌 Ex	pression ⊆lear Apply
No Time Source Destination	Protocol Info
194 76.110539 00:18:fe:84:97:40 Spanning-tree-(for 195 76.156067 HewlettP_75:f3:37 Spanning-tree-(for 196 76.157405 00:18:fe:84:97:40 Spanning-tree-(for 197 76.201596 HewlettP_75:f3:37 Spanning-tree-(for 198 76.22601 00:18:fe:84:97:40 Spanning-tree-(for 199 76.246837 HewlettP_75:f3:37 Spanning-tree-(for 200 76.247966 00:18:fe:84:97:40 Spanning-tree-(for 201 76.293235 00:18:fe:84:97:40 Spanning-tree-(for 202 76.393235 00:18:fe:84:97:40 Spanning-tree-(for 203 76.387517 HewlettP_75:f3:37 Spanning-tree-(for 204 76.391816 00:18:fe:84:97:40 Spanning-tree-(for 205 76.433681 HewlettP_75:f3:37 Spanning-tree-(for 206 76.48162 00:18:fe:84:97:40 Spanning-tree-(for 207 76.480749 HewlettP_75:f3:37 Spanning-tree-(for 207 76.480749 HewlettP_75:f3:37 Spanning-tree-(for 208 76.48163 00:18:fe:84:97:40 Spanning-tree-(for 209 76.524641 HewlettP_75:f3:37 Spanning-tree-(for	EAP Request, PEAP [Palekar] TLS Client Hello EAP Request, PEAP [Palekar] EAP Reguest, PEAP [Palekar] EAP Request, PEAP [Palekar] EAP Response, PEAP [Palekar] EAP Response, PEAP [Palekar] TLS Server Hello, Certificate, Certificate Request, Server Hello TLS Certificate, Client Key Exchange, Change Cipher Spec, Certificate, Client Key Exchange, Change Cipher Spec, Certificate, Cartificate, Change Cipher Spec, Certificate, Cartificate, Car
Length: 6 Type: PEAP [Palekar] (25) Flags(0x0): PEAP version 0	
0000 01 80 c2 00 00 03 00 0e 7f 75 f3 37 88 8e 01 00 0010 00 06 c2 43 00 06 19 00 00 00 00 00 00 00 00 00 0020 00 00 00 00 00 00 00 00 00 00 00 00	
File: "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\etherXXXT6RUUT" 172 KB 00:10:48	P: 653 D: 345 M: 0 Drops: 0

Here we can see the failure is reported at packet 223 (after a delay of 30 seconds). This type of trace would indicate that there is a password mismatch between Jetdirect and the Active Directory account that represents Jetdirect.

Appendix B: Importing a Certificate

Bring up the web server for the CA.





Be sure to		
select the	File Edit View Eavorites Tools Help	
Certificate	Ca Back • ⊙ • R R A Search ☆ Favorites I > 2	-
Template "HP	Address 🗿 http://loopback/certsrv/certrqma.asp	»
Jetdirect" and	Misson Continues Desta	-
to check the	microson centilicate Services - Routca <u>nome</u>	
checkbox	Advanced Certificate Request	
entitled "Mark	Certificate Template:	
keys as	HP.letdirect	
evportable"		
exponable .	Identifying Information For Offline Template:	
	Name: J7961A 000E7FE80157 S/N: SG53302227	
	E-Mail: printeradmin@example.com	
	Company: Example	
	Department: Printing and Imaging	
	City: exampletown	
	State: EX	
	Country/Region: EX	
	Key Options:	
	Create new key set	
	CSP: Microsoft RSA SChannel Cryptographic Provider	
	Key Usage: @ Exchange	
	Key Size: 1024 Min: 1024 (common key sizes: 1024 2048 4096 8192 16384)	
	Automatic key container name Ollser specified key container name	
	✓ Mark kevs as exportable	
	Export keys to file	
	Enable strong private key protection	
	Store certificate in the local computer certificate store Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.	
	Additional Options:	
	Request Format: © CMC © PKCS10	
	Hash Algorithm: SHA.1	
	Only used to sign request.	
	□ Save request to a file	
		-
	Cone	11.
	Only used to sign request. Save request to a file Done Internet Internet	

Click Yes.	Potential Scripting Violation
Check res.	This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you. Do you want to request a certificate now?
	Yes No

Ulick "Install	Misson Cashilisaka Cassings Misson D Takawak Cuslavar	
this certificate"	File Edit View Favorites Iools Help	
to install it on	🔾 Back 🔹 🕤 👻 😰 🐔 🔎 Search Favorites 🧑 🙆 🔹 😓	
your local	Address 🗃 http://loopback/certsrv/certfnsh.asp	💌 🛃 Go 🛛 Links 🌺
, computer. We	Microsoft Cartificate Services PostCA	Home
will export it	History	
and then	Certificate Issued	
delete it from	The certificate you requested was issued to you.	
this computer	Install this sortificate	
later.		
		-
		🔮 Internet 🏼 🎢

	Potential Scripting Violation
Click Yes.	This Web site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data. Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No. Yes Yes



At this point, we want to export the certificate so that it can be loaded with its private key into Jetdirect. We need to bring up MMC again and load the Certificates snap-in.

Go to the File	the Console1			
Menu and	Ele Action View Favgrites Window Help			
select				
Add/Remove	in Console Root			
Snap-In	There are no items to show in this view.			
Shup-in.				
	Add/Remove Snap-in			
Click "Add"	Standalone Eutensions			
	Use this page to add or remove a standalone Snap-in from the console.			
	Snap-ins added to: Console Root 🔍 📰			
	Description			
	Add Remove About			
	Ağu Demove Ağour			
	UK			

Click Certificates"	Add Standalone Snap-in		? ×
Cermicales	Available Standalone Snap-ins:		
	Snap-in	Vendor	
	 NET Framework 1.1 Configuration Active Directory Domains and Trusts Active Directory Sites and Services Active Directory Users and Comput ActiveX Control Authorization Manager Backup Certificate Templates Certification Authority 	Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation	
	Description The Certificates snap-in allows you to brow certificate stores for yourself, a service, or	vse the contents of the a computer. <u>A</u> dd <u>C</u> los	e

Click "My usor	Certificates snap-in
account	This snap-in will always manage certificates for:
	My user account
	C Service account
	C Computer account
	KBack Finish Cancel

Click "Local	Select Computer
Computer"	
	Select the computer you want this snap-in to manage.
	This snap-in will always manage:
	Local computer: (the computer this console is running on)
	Another computer: Browse
	Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.
	< <u>B</u> ack Finish Cancel



The "Certificate	Certificate Export Wizard	×
Export Wizard" launches – Press "Next"	Welcome to the Certific Wizard This wizard helps you copy certificates, lists and certificate revocation lists from store to your disk. A certificate, which is issued by a certifit a confirmation of your identity and cont used to protect data or to establish sec connections. A certificate store is the sycertificates are kept. To continue, click Next.	cate Export certificate trust a certificate cation authority, is cains information ure network ystem area where
	< <u>B</u> ack	Cancel

Since we are going to import this	Certificate Export Wizard X Export Private Key You can choose to export the private key with the certificate.
Jetdirect, we need to export the private key as well. Select "Yes, export the private key" and then click "Next".	Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page. Do you want to export the private key with the certificate? • Yes, export the private key • Ng, do not export the private key • Ng, do not export the private key • Reack • Back • Next >

	Certificate Export Wizard
password to protect the private key.	Password To maintain security, you must protect the private key by using a password.
Click "Next".	Type and confirm a password. Password:
	I ⊆onfirm password: ●●●●●●●●●●
	< <u>B</u> ack Next > Cancel
ame the file	
dcert.pfx″	Certificate Export Wizard
nd click Next″	File to Export Specify the name of the file you want to export
nd click Next″	File to Export Specify the name of the file you want to export Eile name: D:\Documents and Settings\Administrator\Desktop\jdcert.pfx Browse
nd click Next″	File to Export Specify the name of the file you want to export Eile name: D:\Documents and Settings\Administrator\Desktop\jdcert.pfx Browse
nd click Next″	File to Export Specify the name of the file you want to export Eile name: D:\Documents and Settings\Administrator\Desktop\jdcert.pfx Browse
nd click Next″	File to Export Specify the name of the file you want to export Eile name: D:\Documents and Settings\Administrator\Desktop\jdcert.pfx Browse

Click Finish	Certificate Export Wizard
	Completing the Certificate Export Wizard You have successfully completed the Certificate Export Wizard You have specified the following settings: Export Keys Yes Include all certificates in the certification path Yes File Format Person Image: Section of the tertification path Yes Vour News Yes Image: Section of the tertification path Yes Image: Section of tertification path Yes Image: Sectio
Click Ok.	
	Certificate Export Wizard 🔀 The export was successful.

If you did not use the certificate request method of generating a certificate, we'll want to "Import the Certificate and Private Key" into Jetdirect.







© 2016 Copyright HP Development Company, L.P. The information contained in this document is subject to change without notice. HP makes no warranty of any kind with respect to this information. HP specifically disclaims the implied warranty of merchantability and fitness for a particular purpose. HP shall not be liable for any direct, indirect, incidental, consequential, or other damage alleged in conjunction with the furnishing or use of this information.

Microsoft, Windows, and Windows NT/2000/XP/2003/2008/Vista are registered trademarks of Microsoft Corporation in the USA, and other countries. All other brand and product names are trademarks or registered trademarks of their respective companies.