

July 2011 Revision 1.0 © 2015 ZIH Corp. All rights reserved. Zebra and the Stylized Zebra Head are trademarks of ZIH Corp, registered in many jurisdictions worldwide. All other trademarks are property of their respective owners.

Table of Contents

1.	Intro	oduction:	4
	1.1	Overview:	4
	1.2	Applications:	6
	1.3	Restrictions:	6
2.	Pre-	Requisites:	7
	2.1	Requirements:	7
	2.2	Components Used:	7
3.	Con	figuration:	8
	3.1	Generating a Certificate Request:	8
	3.2	Importing Signed Certificates:	12
	3.3	Assigning Trustpoints:	16
4.	Mic	rosoft CA Certificate Request:	19
5.	Refe	erence Documentation:	22

1. Introduction:

1.1 Overview:

Security in 802.11 systems relies on digital certificates to provide mutual authentication and encryption. Mutual authentication or trust is provided by leveraging Public Key Infrastructure (PKI) which allows all parties in the security exchange to verify and validate digital certificates on each party. Authentication and encryption is provided using standard public key and private key algorithms to protect credentials exchanged over the air as well as exchange credentials.



1.1.1 Certification Authority:

To verify that a digital certificate is not forged, you need a mechanism to validate it which is provided by a certification authority (CA). The CA is a trusted third party that can be a private secure server deployed in an enterprise data center or a public server from a specialized company offering certificates such as Entrust, Go Daddy or, VeriSign.

The CA is charged with signing all user and server certificates and signs a certificate by running a hash of the certificate contents, encrypting the hash with its Private Key (creating a digital signature), then appending this signature to the end of the certificate. The CA also has a certificate of its own called a CA certificate or root certificate. The root certificate contains the CA's Public Key and can be freely distributed any party. Anyone that has the CA's root certificate installed can validate certificates issued from the CA.



Most operating systems include root certificates issued from top public certificate providers allowing secure transactions to be made on-line without having to manually install root certificates.

Using a CA to sign user and server certificates and validate them is the simplest form of Public Key Infrastructure (PKI). A certificate chain includes information about the CA or CA's involved in issuing certificates and the user or server certificates themselves. There are other PKI functions such as certificate revocation lists, cross-certification and certificate chaining that are used but are beyond the scope of a guide.

1.1.2 Trustpoints:

Server and CA certificates are installed in pairs on the RF Switch into trustpoints which are assigned to the local RADIUS and HTTPS services. Each service on the RF Switch supports a single trustpoint allowing separate server certificates to be used for RADIUS and HTTPS services.

WiNG provides a default trustpoint which includes a self-signed server certificate which is assigned to the local RADIUS and HTTPS services. However as the default server certificate is self-signed, no mutual authentication can be provided as no Certificate Authority (CA) root certificate exists to allow the end users to trust the self-signed certificate.

To provide mutual authentication and trust for management, EAP and Hotspot services a trustpoint needs to be created on the RF Switch and a certificate request generated to a public or enterprise CA. Once the certificate request has been signed by the CA, the server and CA certificate can be installed on the RF Switch. Once installed the RF Switch mutual authentication can occur between all parties with certificates issued from the CA.

1.1.2.1 Server Certificates:

Server certificates are digital identifications containing information about a server, service or organization. Server certificates contain a public key which is used to create a secure TLS connection between the service and end user device. In WLAN environments server certificates are used to provide secure encrypted HTTPS management connections to RF Switches and Access Points as well as protect credentials over the air for Hotspot and EAP authentication.

Server certificates are required for all external RADIUS servers providing EAP authentication as well as the RF Switches providing RADIUS, Hotspot or secure web based management. The RF Switch supports a single server certificate for local RADIUS services and a single server certificate to provide Hotspot and secure web based management.

1.1.2.2 Root Certificates:

A root certificate is a self-signed certificate or an unsigned public key certificate which forms the foundation of a public key infrastructure (PKI). A root certificate is the top-most certificate in the Certificate Authority (CA) tree, and its private key is used sign all certificates issued from the CA.

Root certificates are installed on end user devices to identify and verify digital certificates issued from CAs. Root certificates for common public CAs such as Entrust and VeriSign are typically pre-installed on most operating systems allowing the end user devices to automatically trust servers and applications using digital certificates issued from these CAs. However in enterprise environments, a private CA is often deployed and CA certificates are automatically or manually distributed to end user devices before certificate verification and trust can occur.

It's not mandatory that a CA root certificate be installed on the end user device for WLAN authentication as web browsers and 802.1X supplicants can establish a secure connection to a peer without a CA certificate being present. However in WLAN deployments it is strongly recommended that a CA root certificate be installed as the CA certificate provides the only mechanism for the end device to verify the identity of the presented digital certificate prior to credentials being exchanged. Without a CA certificate being installed, the device is susceptible to man-in-the-middle (MIN) attacks.

1.2 Applications:

Digital certificates are required to enable the following services on the RF Switch:

- Secure Web UI Management Provides secure remote web based management of the RF Switch. When enabled all web management configuration transactions are encrypted using Transactional Layered Services (TLS). In addition PKI allows the remote management station to verify the identity of the RF Switch prior to submitting management credentials.
- 2) EAP Authentication When using the integrated RADIUS server, PKI allows the RF Switch to authenticate users using PEAP, EAP-TLS and EAP-TTLS. These EAP methods provide mutual authentication between the RF Switch and 802.1X supplicant as well as a secure TLS tunnel to exchange credentials over the air.
- 3) Hotspot Authentication Provides web based authentication for users. When users authenticate to the RF Switch by presenting a username and password which is encrypted over the air using TLS. In addition PKI provides the ability to allow the end user to verify the identity of the RF Switch prior to submitting credentials.

1.3 Restrictions:

A single trustpoint can be assigned to the HTTPS service which is shared for both secure Web-UI management and Hotspot services.

If Hotspot authentication is required, Zebra recommends that the hostname for the CN field in the server certificate be defined to resolve to the IP address assigned to the Hotspot virtual interface. This will ensure compatibility with Mozilla Firefox and Microsoft Internet Explorer which uses the CN field to detect phishing attacks.

2. Pre-Requisites:

2.1 Requirements:

The following requirements must be met prior to attempting this configuration:

One (or more) RF Switches are installed and operational on the network.

One (or more) Access Ports configured and adopted by the RF Switch.

One (or more) WLAN profiles are configured and assigned to adopted radios.

A Windows XP workstation is available with Microsoft Internet Explorer or Mozilla Firefox to perform Web UI configuration.

A public or private Certificate Authority available to issue server certificates to the RF Switch.

The reader has read the Zebra Solutions WiNG 5 System Reference

2.2 Components Used:

The information in this document is based on the following Zebra hardware and software versions:

1 x RFS6000 Version 5.1.0.0-074R.

1 x AP7131N.



Registered users may download the latest software and firmware from the Zebra Solutions Support Site http://support.symbol.com.

3. Configuration:

The following section outlines the configuration steps required to add a Digital Certificate issued from a Certification Authority onto a RF Switch. This guide describes the steps to create a trustpoint on an RFS6000 switch. But the same steps can be used for installing a trustpoint on any other controller or access point.

- 1) Generating Certificate Request [Section 3.1]:
- 2) Importing Signed Certificates [Section 3.2]:
- 3) Assigning Trustpoints [Section 3.3]:

3.1 Generating a Certificate Request:

Before a certificate can be installed into a trustpoint on the RF Switch, a certificate request must be generated. A certificate request will generate a new certificate key and prepare a certificate signing request (CSR) which can be entered into a Certificate Authority to generate a server certificate.

The CSR contains information identifying the RF Switch including information such as Company, Organization, Department, Country and Locality. The CSR also include specific network level information about the RF Switch such as IP Address, hostname and fully qualified domain name.

When a certificate signing request is generated, the RF Switch will generate a Base64 PKCS#10 binary encoded text which can be saved to a file. The PKCS#10 file can then be uploaded to a CA or the PKCS#10 file opened in a text editor and the content copied and pasted into a form on the CA.

----- BEGIN CERTIFICATE REQUEST-----MIIBNTCCAQYCAQAwXTELMAkGA1UEBhMCUOcxETAPBgNVBAoTCEOyQ3J5cHRvMRIw EAYDVQQDEwlsb2NhbGhvc3QxJzAlBgkqhkiG9w0BCQEWGGFkbWluQHNlcnZlci5l eGFtcGxlLmRvbTCBnzANBgkqhkiG9w0BAQEFAA0BjQAwgYkCgYEAr1nYY1Qrll1r uB/FqlCRrr5nvupdIN+3wF7q915tvEQoc74bnu6b8IbbGRMhzdzmvQ4SzFfVEAuM MuTHeybPq5th7YDrTNizKKx0BnqE2KYuX9X22A1Kh49soJJFg6kPb9MJgiZBiMv tb7K3CHfgw5WagWnLl8Lb+ccvKZZl+8CAwEAAaAAMA0GCSqGSIb3DQEBBAUAA4GB AHpoRp5YS55CZpy+wdigQEwjL/wSluvo+WjtpvP0YoBMJu4VMKeZi405R7o8oEwi PdlrrliKNknFmHKIaCKTLRcU59ScA6ADEIWUzqmUzP5Cs6jrSRo3NKfg1bd09D1K 9rsQkRc9Urv9mRBIsredGnYECNeRaK5R1yzp0owninXC

---- END CERTIFICATE REQUEST----

Figure 3.1 – Base64 Encoded CSR Generated from an RF Switch



Section 4.0 explains the process for issuing a server certificate using Microsoft Certificate services

3.1.1 Web UI Configuration Example:

The following configuration example will demonstrate how to create a trustpoint and generate a Certificate Signing Request on the RF Switch using the Web UI:

1) Navigate to the *Configuration > Devices > RFS6000-81-C2-0E > Certificates* window. Click "*Launch Manager*".

Dashboard Configurati	on Diagnostics Operation	ons Sti	atisti	CS 🔷 RF56000	M	WiNG	v5.1	🙎 admin	-
Devices Wireless Pro	files RF Domains Security	Servic	es	Management			5) Revert 🛛 🖄 Commit	Save
Device rfs6000-81C20E	(00-15-70-81-C2-0E) Type	rfs6000							0
Basic Configuration *	Management Security								- ÷
Licenses	HTTPS Trustpoint	Pending	0						
Certificates		Chound	0	Contraction () (-				
v RF Domain Overrides		300100	0	default-trustpoint	Launc	h Manager			
RF Domain	SSH RSA Key	Pending	0						
Sensor Configuration		Church	0		100				
WLAN Override		Stored	•	default_rsa_key		Launch	Manager		
v Profile Overrides	RADIUS Security								
General	RADIUS Certificate Authority	Pending	۲						
Cluster		Stored	0	default-trustpoint	Laune	h Manager			
w Interface									
Ethernet Ports	RADIUS Server Certificate	Pending	0						
Virtual Interfaces		Stored	۲	default-trustooint	Laune	h Manager			
Port Channels	1000								
WAN Backhaul	Information								_
► Network	"Pending" Trustpoints and RSA Keys	have not be	en veri	ified to exist on the device.					
► Security -								OK , Ret	let, Exit

2) In the Certificates Management, select Create CSR tab. Select the option Create New to generate a new RSA Key (private key) to be used with the trustpoint. Enter the key name rfs6000_rsa_key. Set the key size to 1024 bits (default). Select the subject name as user-configured. Enter the required server certificate information that will be forwarded to the certificate authority in the certificate request. The certificate authority will use the information entered on this page to generate the server certificate. Click Generate CSR.

Country (C)	The country to be displayed in the server certificate for identification (example US).
State (ST)	The state or province to be displayed in the server certificate for identification (example CA).
City (L)	The locality or city to be displayed in the server certificate for identification (example San Francisco).
Organisation (O)	The company name or organisation to be displayed in the server certificate for identification (example MSI.).
Organisation Unit (OU)	The organisation or department to be displayed in the server certificate for identification (example WNS).

Common Name (CN)	The hostname of the RF Switch (example rfs6000.Zebrasolutions.com). The common name must be resolvable by DNS to the management or Hotspot interface on RF Switch for the client to trust the certificate.
Email Address	The email address to contact for issues related to the certificate request
IP Address	The IP Address on the device for the management or Hotspot interface using the certificate. The IP Address will be added to the Subject Alternative Name field in the server certificate (example 192.168.10.14).
FQDN	The fully qualified domain name that specifies the node's position in the DNS tree hierarchy.

Certificate Managem	ent			×
Device MAC rfs6000-	81C20E (00-15-70-81-C2-0E	E)		0
Trustpoints	Create New Certificate Signi	ng Request (CSR)		
RSA Keys	RSA Key	• Create New O Use Existing		
🗒 Create Certificate		rfs6000 rsa key 1024	4 (1,024 to 2,048 bits)	
🗔 Create CSR			•	
	Certificate Subject Name –			
	Certificate Subject Name	🚬 🔘 auto-generate		
		user-configured		
	Country (C)	US	S.	
	State (ST)	CA		_
	City (L)	San Francisco		
	Organization (O)	MSI		
	Organizational Unit (OU)	WINS		
	Common Name (CN)	RFS6000		
	Additional Credentials			
	Email Address	sjohar@motorolasolutions.com		
	Domain Name	motorolasolutions.com		
	IP Address	192.168.10.1		
		L		*
			Ge	nerate CSR

3) The RF Switch will generate a Base64 PCKS#10 encoded certificate request that can be entered into a Certificate Authority to generate the server certificate. The certificate request encoded text can be saved to a text file. Click *Close*.



4) The server certificate request can now be injested by a Certificate Authority to generate a server certificate. An example using Microsoft Certificate services is provided in <u>Section 4</u>.

3.1.2 CLI Configuration Example:

1) Enter the following command to generate a certificate request with the parameters explained in step #2 above. The certificate request will be saved into a file csr_req.txt on the TFTP server. The server certificate request can now be injected by a Certificate Authority to generate a server certificate. An example using Microsoft Certificate services is provided in Section 4.

rfs6000-81C20E# crypto pki export request generate-rsa-key rfs6000_rsa_key subject-name RFS6000 US CA "San Francisco" MSI WNS tftp://10.10.1.64/csr_req.txt

3.2 Importing Signed Certificates:

Once a certificate has been issued form a CA, it will need to be imported along with a CA root certificate into the trustpoint on the RF Switch. Most CAs provide the ability to save an issued certificate in numerous formats and care needs to be made to ensure that the issued server and CA root certificates are saved using Base64 encoding. The Base64 encoded server certificate and CA root certificate files can then be uploaded into the RF Switch.

----BEGIN CERTIFICATE----

MI I F1zCCBL+gAwI BAgI KbHnDYwAAAAAAJzANBgkqhki G9w0BAQUFADBBMRMwEQYK CZI mi ZPyLGQBGRYDY29t MRYwFAYKCZI mi ZPyLGQBGRYGZXN1 bGFi MRI wEAYDVQQD Ewl FUOVMQUI gQOEwHhcNMDgwODEOMTg1MDI 4WhcNMTAwODEOMTg1MDI 4Wj B9MQsw CQYDVQQGEwJVUzELMAkGA1UECBMCVE4xFTATBgNVBAcTDEpvaG5zb24gQ2l0eTEW MBQGA1UEChMNTW90b3JvbGEgSW5jLjEhMB8GA1UECxMYRW50ZXJwcmlzZSBXTEF0 I ERpdml zaW9uMQ8wDQYDVQQDEwZ3czYwMDAwgZ8wDQYJKoZI hvcNAQEBBQADgY0A MIGJAoGBALZ+8aJWSJ7JjuVJ7f+iNffacvh+vN44raTFzRUTaDgR04jSqSgA6w8N fPTUVc0xG8sq5Vwg19qi ugcw2H8MDaAI l MAVqdbkccsoLm30l d6YyVI Yf3CvfATW s7p/AWWoIgFtFjc4rAtENPPvyqB/eMSTa8sidgeCCACN4XE1EUVzAgMBAAGjggMX MI I DEZALBgNVHQ8EBAMCBaAwEwYDVROI BAwwCgYI KwYBBQUHAwEwI gYDVRORBBsw GYcEwKgKDoI Rd3M2MDAwLmVzZWxhYi 5j b20wHQYDVR00BBYEFLZMmzI BZj RRUr+o /W3ZVxIRZhA2MB8GA1UdIwQYMBaAFPq5zcZQepfvVBYM8C+DAifE03XUMIIBBAYD VROFBI H8MI H5MI H2oI HzoI HwhoGObGRhcDovLy9DTj 1FUOVMQUI l Mj BDQSxDTj 13 M2tzZXJ2ZXI xLENOPUNEUCxDTj 1QdWJsaWM Mj BLZXkl Mj BTZXJ2aWNl cyxDTj 1T ZXJ2aWNl cyxDTj 1Db25maWd1cmF0aW9uLERDPWVzZWxhYi xEQz1j b20/Y2VydGl m aWNhdGVSZXZvY2F0aW9uTG1 zdD9i YXN1 P29i amVj dENsYXNzPWNSTERpc3RyaWJ1 dGl vbl BvaW50hj dodHRw0i 8vdzNrc2VydmVyMS5l c2VsYWI uY29tL0Nl cnRFbnJv bGwvRVNFTEFCJTI wQOEuY3JsMI I BGQYI KwYBBQUHAQEEggELMI I BBzCBqQYI KwYB BQUHMAKGgZxsZGFw0i 8vL0N0PUVTRUxBQi UyMENBLEN0PUFJQSxDTj 1QdWJsaWM Mi BLZXkl Mi BTZXJ2aWNl cyxDTj 1TZXJ2aWNl cyxDTj 1Db25maWd1cmF0aW9uLERD PWzZWxhYi xEQz1j b20/Y0FDZXJ0aWZpY2F0ZT9i YXNl P29i amVj dENsYXNzPWNl cnRpZml j YXRpb25BdXRob3JpdHkwWQYI KwYBBQUHMAKGTWhOdHA6Ly93M2tzZXJ2 ZXI xLmVzZWxhYi 5j b20vQ2VydEVucm9sbC93M2tzZXJ2ZXI xLmVzZWxhYi 5j b21f RVNFTEFCJTI wQOEuY3JOMAwGA1UdEwEB/wQCMAAwOwYJKwYBBAGCNxUHBC4wLAYk KwYBBAGCNxUInfYig5iFL4flkyuZ1FSErMwMgRSEtrkpt5s4AgFkAgEDMBsGCSsG AQQBgj cVCgQOMAwwCgYI KwYBBQUHAwEwDQYJKoZI hvcNAQEFBQADggEBAGmLi 8TT R2fi 83zBKI rbED30f+l ZvU6MmotL40Pi dNi StvVxCFpCWzYuneVYpdRXAYabv4H5 5XKl zgx0n/FJuI Xv5mj GG7M4mI vLF1CAfXj YAI cqBK2U9no9bf5g9ySPocCGEbK/ mB64HHAeYEVcCHi Hr4Qcq6XtKWE6SL2mYZxTB8a3abNAy0zcqpI s9GkcW1mi Vi IX g1RpwRYX5wi 8Ql EPtF08j cqUbGj wBx0tI 6TzkB+U0pPp8i k2TXg+nNGKExzxFD7V Ki Sen5RS3YyCAStrQCUzzfjH8WZ6Aq7hgiBSbJMte2W/JzH0hwhmuexX3g9K60hH 04xZS4gHW03qc8Y=

---- END CERTI FI CATE-----

Figure 3.2 – Base64 Encoded Certificate Issued from a CA

3.2.1 Web UI Configuration Example:

The following configuration example will demonstrate how to ingest a server and CA root certificate issued from a CA into a trustpoint on an RF Switch using the Web UI:

1) Navigate to the *Configuration > Devices > RFS6000-81C2 > Certificates window.* Click *Launch Manager*.

Dashboard Configuration	Diagnostics Operations Statistics 🔷 🌆	ᄊ WING v5.1 🚨 admin 🛛
Devices Wireless Profiles	RF Domains Security Services Management	5) Revert 🔥 Commit 🔚 Save
Device rfs6000-81C20E (00-1	5-70-81-C2-0E) Type rfs6000	0
Basic Configuration Amar Licenses	agement Security	-
Certificates	Stored ③ default-trustpoint ▼	Launch Manager
FF Domain Overrides RF Domain Sensor Configuration WLAN Override	SHRSA Key Pending O Stored O default_rsa_key	Launch Manager
v Profile Overrides RAD	US Security	
General R	ADIUS Certificate Authority Pending	
w Interface	Stored Udefault-trustpoint *	Launch Manager
Ethernet Ports R	ADIUS Server Certificate Pending	
Port Channels WAN Backhaul	Stored default-trustpoint finformation ing* Trustpoints and RSA Keys have not been verified to exist on the device.	Launch Manager
► Security -		OK , Reset, Exit

2) To create a new trustpoint, select the *Trustpoints* tab and click *Import CA*.

Certificate Managem Device MAC rfs6000-	ent 81C20E (00-15-70-81-C	:2-0E)	×				
Trustpoints	default-trustpoint	Certificate Details					
🕎 RSA Keys 📆 Create Certificate		Subject Name	C=US, ST=CA, L=San Jose, O=Enterprise Mobility, OU=EWLAN, CN=Motorola				
🕎 Create CSR		Alternate Subject Name	A				
		Issuer Name	C=US, ST=CA, L=San Jose, O=Enterprise Mobility, A OU=EV/LAN, CN=Motorola				
		Serial Number	034b				
		RSA Key Used	default-trustpoint-srvr-priv-key				
		IS CA	×				
		Is Self Signed	✓				
		Server Certificate Present	✓				
		CRL Present	×				
		Validity					
		Valid From	12:28:2010 16:42:21 UTC				
		Valid Until	12:28:2011 16:42:21 UTC				
		Import Import C	CA Import CRL Import Signed Cert Export Delete				

3) In the Trustpoint name enter a unique trustpoint name *rfs6000_trustpoint* for the trustpoint where the server certificate and the CA certificates will be associated. Select the *Cut and Paste* button to copy the Base 64 encoded CA Root Certificate issued from the Certificate Authority. Click *Ok*.

Import CA Certificate	0
	•
Signed Certificate Details	
Trustpoint Name 😽 rfs6000_trustpoin1	
Location of Signed Certificate	
From Network Cut and Paste	
BEGIN CERTIFICATE	
MIIEejCCA2KgAwlBAglQYIsUgc5zKqtIskgy7ofgdj	
ANBgkqhkiG9w0BAQUFADBD	
MRMwEQYKCZImiZPyLGQBGRYDY29tMRcwFQY	
KCZImiZPyLGQBGRYHc3ltYm9sczET	
MBEGA1UEAxMKc3ltYm9scy5DQTAeFw0xMDA5	
MjcwODE4MjZaFw0xNTA5MjcwODly	
NDIaMEMxEzARBgoJkiaJk/IsZAEZFgNjb20xFzAV	
BgoJkiaJk/IsZAEZFgdzeW1i	
p2xzMRMwEQYDVQQDEwpzeW1ib2xzLkNBMIIBlj	
ANBgkqhkiG9w0BAQEFAAOCAQ8A	
MIIBCgKCAQEA4bcYQ7wDFHxVssKzu1L+3hw5 🥊	
	OK Count

4) To import the signed certificate, click *Import Signed Certificate.*

Trustpoints	🗔 default-trustpoint	Certificate Details					
🗔 RSA Keys		Subject Name	C=US, ST=CA, L=San Jose, O=Enterprise Mobility, OU=EVLAN, CN=Motorola				
Create CSR		Alternate Subject Name					
		Issuer Name	C=US, ST=CA, L=San Jose, O=Enterprise Mobility, OU=EV/LAN, CN=Motorola				
		Serial Number	034b				
		RSA Key Used	default-trustpoint-srvr-priv-key				
		IS CA	×				
		Is Self Signed	4				
		Server Certificate Present	4				
		CRL Present	×				
		Validity					
		Valid From	12:28:2010 16:42:21 UTC				
		Valid Until	12:28:2011 16:42:21 UTC				

5) In Certificate name, enter the name of the trustpoint created in step 3.

	^
mport Signed Cert Device MAC 00-15-70-81-C2-0E	0
Import Signed Certificate	
Certificate Name 😽 rfs6000 trustpoint	
Location of Certificate	
From Network Cut and Paste	
BEGIN CERTIFICATE	
MIIFeTCCBGGgAwiBAgIKVY+7aQAAAAAACTAN	
BgkqhkiG9w0BAQUFADBDMRMwEQYK	
CZImiZPyLGQBGRYDY29tMRcwFQYKCZImiZPyL	
GQBGRYHc3ttYm9sczETMBEGA1UE	
AxMKc3ttYm9scy5DQTAeFw0xMTA3MDcxNTixN	
ThaEw0xMzA3MDYxNTlxNThaMGAx	
CZAJBgNVBAYTAIVTMQswCQYDVQQIEwJDQTE	
CZAJBgNVBAYTAIVTMQswCQYDVQQIEwJDQTE VMBQGA1UEBxMNU2FuIEZyYVV5jaXNj	
CZAJBgNVBAYTAIVTMQswCQYDVQQIEwJDQTE VMBQGA1UEBxMNU2FuIEZyYVV5jaXNj bzEMMAoGA1UEChMDTVNJMQwwCqYDVQQLE	
CZAJBgNVBAYTAIVTMQswCQYDVQQIEwJDQTE VMBQGA1UEBxMNU2FuIEZyYVV5jaXNj bzEMMAoGA1UEChMDTVNJMQwwCgYDVQQLE wNXTIMxEDAOBgNVBAMTB1JGUzYwMDAw	

6) The **CA Root Certificate** and the **signed server certificate** is now installed in the trustpoint **rfs6000_trustpoint**. Click **Commit** and **Save** to apply and save changes.

Dashboard Configuration	Diagnostics	Operations Statistics	🤝 RESSING 📈 WING vs.1 🚨 admin 🏼 🤧
Devices Wireless Profile	RF Domains	Security Services Management	5 Revert 🔮 Commit

3.2.2 CLI Configuration:

// Import the CA certificate cacert.cer into rfs6000_trustpoint
rfs6000-81C20E#crypto pki authenticate rfs600_trustpoint tftp://10.106.6.143/cacert.cer

// Import the signed certificate server_cert.cer into rfs6000_trustpoint
rfs6000-81C20E#crypto pki import certificate rfs6000_trustpoint
tftp://10.106.6.143/server_cert.cer

3.3 Assigning Trustpoints:

Trustpoints contain both the server and CA root certificates and can be assigned to the internal RADIUS and HTTPS services on the RF Switch. Flexibility is provided allowing the RF Switch to use a single trustpoint for management, RADIUS and Hotspot services, or two trustpoints can be used with one trustpoint servicing RADIUS and the second trustpoint servicing management and Hotspot users.

3.3.1 Web UI Configuration Example:

The following configuration example will demonstrate how to configure the RF Switch to use the trustpoint configured in sections 3.1 for RADIUS and HTTPS services using the Web UI:

 Navigate to the Configuration > Devices > RFS6000-C20E > Certificates window. Select the rfs6000_trustpoint for Radius Certificate Authority and Radius Server Certificate to be used by the local RADIUS server on the device for EAP Authentication. Click OK and Exit.

Basic Configuration	Management Security							
Licenses Certificates	HTTPS Trustpoint	F	Pending Stored	0		L numah Ma		
🔻 RF Domain Overrides			310164	0	detault-trustpoint		nager	
RF Domain	SSH RSA Key	F	Pending	0	-			
Sensor Configuration WLAN Override		0	Stored	۲	default_rsa_key	•	Launch Manager	
▼ Profile Overrides	RADIUS Security							
General	RADIUS Certificate Authority	F	Pending	0				
Cluster			Stored	•	default-trustpoint	Launch Ma	nager	
► Interface					rfs6000_trustpoint	<u></u>		
▶ Network	RADIUS Server Certificate	F	Pending	0	default-trustpoint			
▶ Security		1	Stored	\odot	default-trustpoint	Launch Ma	nager	
Services	Information				l,	<u> </u>		
Management	"Pending" Trustpoints and RSA Ke	eys hav	ve not be	en vei	ified to exist on the device.			
P Auvanceu	And a second							

Device IIS6000-81C20	E (00-10-70-01-02-0E) Type	# NS600	1				V
Basic Configuration	Management Security						
Licenses	HTTPS Trustpoint	Pendin	g ()				
Certificates		Stored	\odot	default-trustpoint	Launch	Manager	
RF Domain Overrides					[
RF Domain	SSH RSA Key	Pendin	g O				
Sensor Configuration		Stored	•	alafarilli saa linir		Launah Managar	
WLAN Override		010100	0	uerauit_rsa_key	•	Launen Manager	
Profile Overrides	RADIUS Security						
General	RADIUS Certificate Authority	Pendin	g 🔾]			
Cluster		Stored	\odot	default-trustpoint 🔻	Launch	Manager	
► Interface					L		
Network	RADIUS Server Certificate	Pendin	g O	Mot_trustpoint			
▶ Security		Stored	\odot	default-trustpoint 🔻	Launch	Manager	
Services	The second second			rfs6000_trustpoint			
▶ Management				default-trustpoint			
Advanced	"Pending" Trustpoints and RSA Ke	ys have not	been ve	ified to exist on the device.			
						» ок	Reset Exit

 Navigate to the Configuration > Devices > RFS6000-C20E > Certificates window. Select the rfs6000_trustpoint to be used for HTTPS, for management access and Hotspot authentication. Click OK and Exit.

	Management Security						
Licenses	HTTPS Trustpoint	Pending	0				
Certificates		Stored	•	aladar di Amerika aint	Launah	Managar	
🔻 RF Domain Overrides		C.C.C.G.	0	rte6000 tructocint	Launch	Mallager	
RF Domain	SSH RSA Key	Pending	0	default-trustpoint			
Sensor Configuration		Chavad	0				
WLAN Override		Stored	•	default_rsa_key	•	Launch Manager	
Profile Overrides	RADIUS Security						
General	RADIUS Certificate Authority	Pending	0				
Cluster		Stored	\odot	default-trustnoint	Launch	Manager	
► Interface			-				
▶ Network	RADIUS Server Certificate	Pending	0	Mot_trustpoint			
▶ Security		Stored	•		Launch	Manager	
Services	and a second		0	derduk-trastpoint +	Luditon	miniger	
▶ Management	Juformation						
Advanced	"Pending" Trustpoints and RSA Ke	ys have not be	en ver	ified to exist on the device.			

3) Click **Commit** and **Save** to Apply and save changes.



3.3.2 CLI Configuration:

rfs6000-81C20E*# Enter configu rfs6000-81C20E(co rfs6000-81C20E(co https radius-ca radius-serve	configure terminal uration commands, one per line. End with CNTL/Z. onfig)*#rfs6000 00-15-70-81-C2-0E onfig-device-00-15-70-81-C2-0E)#trustpoint ? Assign the trustpoint to HTTPS Assign the trustpoint to be used as certificate authority, for validating client certificates in EAP er Assign the trustpoint for radius server certificate
WORD Tru	stpoint name; this should be installed on the device using PKI commands in enable mode
rfs6000-81C20E(c rfs6000-81C20E(c rfs6000-81C20E(c	onfig-device-00-15-70-81-C2-0E)#trustpoint radius-ca rfs6000_trustpoint onfig-device-00-15-70-81-C2-0E)#trustpoint radius-server rfs6000_trustpoint onfig-device-00-15-70-81-C2-0E)#trustpoint https rfs6000_trustpoint

4. Microsoft CA Certificate Request:

The following demonstrates the certificate request process on a Microsoft Windows Server 2003 Enterpriser Edition Server running Microsoft Certificate Services as an Enterprise Root CA:

1) Using Microsoft Internet Explorer connect to the Certificate Services web enrollment tool and authenticate using the administrator username and password. The default URL to access the web enrollment tool is *http://servername/CertSrv*.

C C T I http://w3kserver1.eselab.com/CertSrv	▼ + ₇ ×
2) Select <i>Request a certificate</i> .	
Microsoft Certificate Services ESELAB CA Welcome Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you car identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificat perform other security tasks. You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation lisview 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 or a pending certificate request	Home n verify your te you request, st (CRL), or to

3) Select advanced certificate request.

Request a Certificate	
Select the certificate type: <u>User Certificate</u>	
Or submit an advanced certificate request	

4) Select Submit a certificate request by using a base-64-encoded CMC or PKCS#10 file, or submit a renewal request by using a base-64-encoded PKCS#7 file.

Microsoft Certificate Services ESELAB CA	<u>Home</u>
Advanced Certificate Request	
The policy of the CA determines the types of certificates you can request. Click one of the following options to:	
Create and submit a request to this CA.	
Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-enc PKCS #7 file.	<u>coded</u>
Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station. Note: You must have an enrollment agent certificate to submit a request on behalf of another user.	

5) In the **Base-64-encoded certificate request (CMC or PKCS#10 or PKCS#7)** field, paste the base64 encoded text contained in the certificate request file generated by the RF Switch. In the **Certificate Template** window select a template to use to generate the Server Certificate. In this example a pre-installed template named **Web Server** is used. Click **Submit**.

To submit a sav	ed request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request	
Several Democratic	extential source (such as a web server) in the Saved Request box.	
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	BEGIN CERTIFICATE REQUEST MIICQDCCAakCAQAwgYkxCzAJBGNVBAYTAIVTHQsw SxHEsmobohNvbiBbaXKSHNYWF XTDVQCKE bINJSRv ZxHEsmoLongyXNIIFAUQ4gGC12aXUNDb24xCzAZ OFFILmNvbTCBnzANBgkqhkiG9wDBAQEFAAOBjQAw HaNdzXfO+jz9KOIEhpAHmucNotkH/yTjXgpOKBP ▼ Mowse for a file to insert.	
<u>Certificate Templ</u>	Web Server	
Additional Attribu	les:	
Attributes:		
	Submit >	

6) Select the certificate format Base 64 encoded then click Download certificate. Name the certificate servercer.cer and save the Server Certificate to a location that can be easily accessed so it can be installed on the RF Switch.

Certificate Issued		
he certificate you r	equested was issued to you.	
ODER	ancoded or Sase 64 encoded	
Downlog	d certificate	

7) Click *Home* to access the web enrollment home page then click *Download a CA certificate, certificate chain or CRL*.

<i>Microsoft</i> Certificate Si Welcome	MICES ESELABICA	Ho
Jse this Web site to dentity to people yo perform other securi	request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your u communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you requ y tasks.	∍st,
You can also use this	Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or ending request.	to
For more information	about Certificate Services, see Certificate Services Documentation.	
Select a task: Request a certific	ate	
View the status of Download a CA of	a pending certificate request ertificate, certificate chain, or CRL	

8) Select the Encoding method *Base 64* then click *Download CA certificate*. Name the certificate *caroot.cer* and save the CA Certificate to a location that can be easily accessed so it can be installed on the RF Switch.

M1crosoh Cert1ficate Serv1ces- ESELAB CA	Home
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:	
Encoding method: © Base 64 Download CA certificate Download CA certificate shain Download latest base CRL Download latest delta CRL	

5. Reference Documentation:

Description

Zebra Solutions WiNG 5 System Reference Guide

Zebra Solutions WiNG 5 CLI Reference Guide

Location

http://support.symbol.com

http://support.symbol.com