EMC® Secure Remote Support
Security Management and Certificate Policy

Release 2.00

Frequently Asked Questions

P/N 300-012-181
REV 03

EMC Corporation
Corporate Headquarters:
Hopkinton, MA 01748-9103
1-508-435-1000
www.EMC.com

Published December, 2012

Contents

Preface

Chapter 1 ESRS Benefits

ESRS Benefits 11

Chapter 2 ESRS FAQ

Frequently Asked Questions about EMC Secure Remote Support 14

What is EMC Secure Remote Support? 14
Is the ESRS Gateway Client the same as the ESRS Gateway? .. 14
What EMC products are supported by the ESRS Gateway Client? 14
What is the Policy Manager? 14
Where should the ESRS Gateway client servers be placed in the customer's network environment? 15
How are remote support sessions initiated? 15
How are communications from ESRS secured and encrypted? 16
Why did EMC select Transport Layer Security as its encryption protocol? 16
Does the ESRS client connect the customer's network or storage devices to the Internet or to EMC's network? 16
Is EMC able to access the customer's internal network via the ESRS Client? 16
Is a log of service events and remote sessions maintained? . 17
Can the customer co-locate the Policy Manager application on either a ClarAlert server or a CLARiiON Management

server? 17
What are the required specifications for the customer-supplied server(s) where the ESRS Gateway Client software will reside? 17
What access does EMC have to the ESRS Gateway Client and Policy Manager servers? 18
How do I order the Secure Remote Support? 18
Where can I find more information about ESRS? 19

Chapter 3 ESRS Certificate Policy

Introduction 22
General Provisions 23
Disclaimers of Warranties and Obligations 23
Subscriber Obligations 23
Publication and Repository 23
Liability, Fees & Financial responsibility 23
Compliance audit 23
Operational Requirements 24
Need for Names to Be Meaningful 24
Uniqueness of Names 24
Lifetime of Issued Credential 24
Revocation 24
End-User Private Key Protection 24
Certificate Profiles and Attributes for ESRS2CA 25
Security audit procedures 27
Types of event recorded 27
Frequency of processing log 27
Retention period for audit log 27
Physical, Procedural and Personnel Security 28
Site Location, Construction and Physical Access 28
Trusted Roles 28
Background, Qualifications, Experience, and Clearance 28
Technical Security Controls 29
Public Key Delivery to Certificate Issuer 29
Network Security Controls 29
CA Private Key Protection 29
Life-Cycle Security Assurance 29
Compromise and Disaster Recovery 29
Contact Details 29

Chapter 4 ESRS Security FAQ

Certificates and Encryption 32
Is the connection from the ESRS gateway to EMC mutual SSL authentication? 32
How does the Certificate enrollment work? 32
Self-signed certificates take away the trusted authentication mechanism that verification by a trusted third party provides 33
Is there any type of finger print check carried out on the certificate? 33
Can a certificate be authenticated as being from a certain device and if so how? 33
What is the Certificate life cycle? 33
Can the key life be specified? 34
If a key is compromised what is the revocation procedure? 34
What is the RSA token used for? 34
Are the keys generated added to an EMC key store (web of trust)? 34
Communications 35
What data is sent from the customer to EMC? 35
Is the connection from the External gateway to the device a new tunnel, or does it route straight through to the end device? 35
Does the traffic that is being sent over the internal network need to be encrypted. 35
Does the XML and SOAP conform to industry standards, and is the specification published? 35
What data can an EMC support person see on the customer device? Can the blocks be copied? 36
Packet sizes of Heart beat packets? 36
What ports and protocols will ESRS use? 36
Policy Manager 36
Who is supporting this application? 36
What version of Apache Tomcat is the Policy Manager running? 36
What version of the HSQLDB is the Policy Manager running? 36
Will Patching of the Policy Manager cover issues surrounding Tomcat and HSQLDB? 37
Will EMC notify of vulnerabilities in Tomcat and HSQLDB?.. 37
Why can the logging be recorded on a remote machine? 37
Remote management 37
What remote software is installed? 37

Solution can provide up to twenty concurrent connections how are they to be managed? 37
Termination of sessions? 37
Tracking of EMC users on line? 37
Can the Policy Manager / ESRS Client terminate remote support sessions if they have been inactive for a period of time? 38
Can a customer's support person shadow the session?..... 38
Customer environment 38
Is the ESRS client running as a system service level within the OS? 38
Where are details for patch management (OS and application) and methods to monitor vendor notification? . 38
Policy Manager communicates to ESRS gateway over HTTP port 8090. What is this used for and can it be done over SSL? 38
Can the ESRS be locked down to only communicate with specific EMC IP addresses? 39
Testing 39
Is documentation available to describe the ESRS test environment and the belief in testing in a live environment? . 39

Preface

As part of an effort to improve and enhance the performance and capabilities of its product line, EMC from time to time releases revisions of its hardware and software. Therefore, some functions described in this guide may not be supported by all revisions of the software or hardware currently in use. For the most up-to-date information on product features, refer to your product release notes.

If a product does not function properly or does not function as described in this guide, please contact your EMC representative.

Audience

This guide is intended for customers who are upgrading from EMC Secure Remote Support Gateway (ESRS1) to EMC Secure Remote Support (ESRS2) and have questions about the changes in security management and certificate policy.

Readers of this guide are expected to be familiar with the following topics:

- Local network administration
- Internet protocols and ports
- EMC storage system administration

Conventions used in this guide

EMC uses the following conventions for notes, cautions, warnings, and danger notices.

Note: A note presents information that is important, but not hazard-related.

CAUTION

A caution contains information essential to avoid data loss or damage to the system or equipment.

IMPORTANT

An important notice contains information essential to operation of the software.

Typographical conventions

EMC uses the following type style conventions in this document:

Normal	Used in running (nonprocedural) text for: • Names of interface elements (such as names of windows, dialog boxes, buttons, fields, and menus) • Names of resources, attributes, pools, Boolean expressions, buttons, DQL statements, keywords, clauses, environment variables, filenames, functions, utilities • URLs, pathnames, filenames, directory names, computer names, links, groups, service keys, file systems, notifications
Bold	Used in running (nonprocedural) text for: • Names of commands, daemons, options, programs, processes, services, applications, utilities, kernels, notifications, system call, man pages Used in procedures for: • Names of interface elements (such as names of windows, dialog boxes, buttons, fields, and menus) • What user specifically selects, clicks, presses, or types
Italic	Used in all text (including procedures) for: • Full titles of publications referenced in text • Emphasis (for example a new term) • Variables
`Courier`	Used for: • System output, such as an error message or script • URLs, complete paths, filenames, prompts, and syntax when shown outside of running text

Courier bold	Used for: • Specific user input (such as commands)
Courier italic	Used in procedures for: • Variables on command line • User input variables
< >	Angle brackets enclose parameter or variable values supplied by the user
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections - the bar means “or”
{ }	Braces indicate content that you must specify (that is, x or y or z)
...	Ellipses indicate nonessential information omitted from the example

Where to get help

EMC support, product, and licensing information can be obtained as follows.

Product information — For documentation, release notes, software updates, or for information about EMC products, licensing, and service, go to the EMC Powerlink website (registration required) at:

http://Powerlink.EMC.com

Technical support — For technical support, click Support on the EMC Powerlink home page. To open a service request through Powerlink, you must have a valid support agreement. Please contact your EMC sales representative for details about obtaining a valid support agreement or to answer any questions about your account.

Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Please send your comments regarding this document to:

techpubcomments@EMC.com

1

ESRS Benefits

This chapter describes the customer benefits of EMC Secure Remote Support (ESRS).

Topics include:

- ESRS Benefits 11

ESRS Benefits

EMC® Secure Remote Support (ESRS) is an IP-based automated connect home and remote support solution. ESRS creates both a unified architecture and a common point of access for remote support activities performed on your EMC product.

The ESRS provides the following benefits:

- Provides 24x7 monitoring, diagnosis, and repair of minor EMC hardware issues.
- Uses leading-edge encryption, authentication, audit, and authorization for ultra-high security remote support.
- Addresses compliance with corporate and governmental regulations with logs of all access events.
- Provides easy integration and configuration with your storage management network and firewalls.
- Provides maximum information infrastructure protection. IP-based sessions enable fast information transfer and resolution.
- Consolidates remote support for your EMC information with the ESRS Gateway Client.

- Provides failover protection.
- Provides remote access to your disaster recovery site makes recovery from unplanned events seamless.
- The EMC Policy Manager puts you in complete control and provides the information you need to stay there.
- Protects information in motion or rest. AES256 encryption during information transfer keeps your information yours.
- Reduces costs and data center clutter. Accelerates time to resolution and elimination of modem/phone line costs translates to lower costs.

Note: EMC Secure Remote Support Technical Documentation is available on the EMC Powerlink® website.

2

ESRS FAQ

This chapter provides answers to frequently asked questions about EMC Secure Remote Support (ESRS). Topic includes:

- Frequently Asked Questions about EMC Secure Remote Support . 14

Frequently Asked Questions about EMC Secure Remote Support

What is EMC Secure Remote Support?

EMC Secure Remote Support (ESRS) is EMC's IP-based remote support solution. The naming has been updated slightly in line with naming refinements aimed at driving consistency to the overall EMC Secure Remote Support portfolio. ESRS provides customers with the most secure method of enabling remote connectivity with EMC.

Is the ESRS Gateway Client the same as the ESRS Gateway?

Currently ESRS is implemented on a dedicated gateway server now referred to as the ESRS Gateway Client. The ESRS Gateway Client is very similar to the solution previously referred to as "ESRS Gateway" in that both are configurations that require the software application to be installed on a customer-provided server or VMware instance. There are also ESRS Device Clients where the software application will reside directly on the EMC device rather than the customer-provided server/VMware instance. These ESRS Device Clients are device dependent and utilize the same security structures as the ESRS Gateway Client.

What EMC products are supported by the ESRS Gateway Client?

Products are continually added with each release of the ESRS Gateway Client. For complete details on products and application releases supported by ESRS, refer to the *EMC Secure Remote Support Technical Description* located on EMC Powerlink at Home > Support > Technical Documentation and Advisories > Software ~ S ~ Documentation > Secure Remote Support > Secure Remote Support (ESRS 2) > Technical Notes/Troubleshooting.

What is the Policy Manager?

The Policy Manager is an ESRS application used by customers to control EMC's remote support activity. It does not need to reside on a dedicated server, but can be installed on any server that has network connectivity to the ESRS Client. Even though the Policy Manager is optional, EMC strongly recommends customers install one to provide

access authorization and audit log capabilities, even if they are not immediately required by Customer business processes.

The Policy Manager allows customers to:

- Review audit log for any recent remote support activity or management changes to the Policy Manager configuration.
- View and change the policy settings for any of the managed EMC storage devices.
  - Always allow
  - Never allow
  - Ask for approval
- View and approve pending requests from EMC to access a device (if policy is set to ask for approval).
- Terminate remote sessions.
- Set up secure communication between Policy Manager and client.
- Set up secure communication between Policy Manager and customer Policy Manager users.

Where should the ESRS Gateway client servers be placed in the customer's network environment?

The ESRS Gateway client servers can be placed at any customer-approved location as long as it can communicate with EMC over ports 443 and 8443 outbound (proxies are supported) and with the Policy Manager. The Gateway server(s) can be located in the customer's DMZ, a dedicated storage VLAN or elsewhere on the internal LAN according unique customer security policies. The Policy Manager should be located on the internal LAN.

How are remote support sessions initiated?

As part of the normal ESRS Heartbeat process, any pending work requests (such as remote support session requests) are retrieved by the customer's ESRS client. The ESRS client will log the work request and query the Policy Manager for any rules regarding the request. If the Policy Manager has "always allow" policies, the remote access session request will proceed. As part of this process, the identities of ESRS client and the EMC Enterprise are verified using the SSL/TLS

authentication protocol. If the certificates fail to match, the connection will not be established.

Note: For additional security, all remote support sessions are initiated outbound, via ports 443 and 8443, from the customer's ESRS client. The connection exists only between the ESRS Global Access Server and the customer's ESRS client. EMC's internal network is not attached to the customer's internal network and the ESRS client will never accept incoming session requests.

How are communications from ESRS secured and encrypted?

Communication is IP-based over a Transmission Control Protocol (TCP) network, uses Transport Layer Security Virtual Private Network (TLS VPN), is encrypted using Advanced Encryption Standard (AES)-256 algorithm. In addition, all communication with EMC back-end systems is client-server-authenticated TLS via a public/private certificate key exchange.

Why did EMC select Transport Layer Security as its encryption protocol?

TLS VPN is an industry standard protocol used for managing the security of message transmission across the Internet. TLS VPN provides better security than IPSec VPN for remote access and is easier to deploy because there is no need to manage and support client side VPN software. Additionally, TLS VPN is used to provide access at the application layer, whereas IPSec VPN creates a network-level connection.

Does the ESRS client connect the customer's network or storage devices to the Internet or to EMC's network?

No. Firewalls and either a private network or Virtual LAN (VLAN) keeps customer's storage and network separate from the Internet. All communications are outbound from the customer site to EMC back-end. ESRS Client uses port(s) 443 and/or 8443 outbound only.

Is EMC able to access the customer's internal network via the ESRS Client?

No. EMC can only access specific target devices that have been explicitly approved by the customer. ESRS Client maps devices to

specific IP address and ports on the target device that have been allowed through the internal firewall by the network administrator. Since all communication originates from the customer ESRS client (HTTPS outbound), EMC cannot initiate a remote access session without the ESRS client processing the request and the customer approving the request (if configured to do so within the Policy Manager).

Is a log of service events and remote sessions maintained?

Yes. The optional Policy Manager software installed at the customer site maintains an audit log containing:

- Date and time of event or access
- Serial number of device accessed
- Remote support application used
- EMC service engineer user id or partner ID of individual accessing the device
- Service request number and included notes (if supplied), the policy applied, and whether the request was approved, or denied by timeout

The Policy Manager has the capability to also stream the Audit Logs to a syslog server in the customer's environment. EMC also maintains a detailed audit log on the EMC backend application system tracking all Gateway status messages, file transfers, and remote access session requests.

Can the customer co-locate the Policy Manager application on either a ClarAlert server or a CLARiiON Management server?

Yes, as long as the server meets the minimum hardware and software requirements and the Gateway server can communicate with the system where the Policy Manager is installed. Co-locating is not the recommended configuration, but it is a supported option.

What are the required specifications for the customer-supplied server(s) where the ESRS Gateway Client software will reside?

For the most current information on hardware/software requirements for the ESRS Gateway Client server(s), see the *ESRS Site*

Planning Guide located on EMC Powerlink at Documentation and Advisories > Software ~ S ~ Documentation > Secure Remote Support > Secure Remote Support (ESRS 2) > Installation/Configuration.

What access does EMC have to the ESRS Gateway Client and Policy Manager servers?

The ESRS Client and Policy Manager are not accessible to EMC. The only access EMC has to the ESRS Client is via the execution of remote support diagnostic scripts, which are part of the ESRS Client code. These scripts are used to collect Gateway Client diagnostic information for troubleshooting ESRS Client issues. The customer may configure their Policy Manager to allow "ask for approval" or disallow the execution of the diagnostic scripts. However, this is NOT a recommended practice as it will severely impact troubleshooting of the ESRS Client.

How do I order the Secure Remote Support?

Via Direct Express using part number ESRS GW 200. There is no charge.

Where can I find more information about ESRS?

Additional information is available on EMC Powerlink at the following locations:

- Home > Services > Global Services Offerings > Customer Support Services > EMC Secure Remote Support > EMC Secure Remote Support
- Documentation and Advisories > Software ~ S ~ Documentation > Secure Remote Support > Secure Remote Support (ESRS 2)

If you have questions, contact the TCE Pre-Sales Support Center at 1-866-EMC-7777 (U.S. and Canada), 1-508-435-1000, ext. 54777 (international), or via the Web at:

http://tcepresalessupport.corp.emc.com/

3

ESRS Certificate Policy

This chapter contains the EMC Secure Remote Support Certificate Practice Statement (CPS) and Policy for EMC Corporation's (EMC) Internal ESRS2CA. Topics include:

- Introduction 22
- General Provisions 23
- Operational Requirements 24
- Security audit procedures 27
- Physical, Procedural and Personnel Security 28
- Technical Security Controls 29
- Contact Details 29

Introduction

This is the Certificate Practice Statement (CPS) and Policy for EMC Corporation's (EMC) Internal ESRS2CA. This Certificate Authority (CA) functions as a standalone CA and is not chained to any commercially trusted public CA.

This statement defines the policies and procedures followed by EMC Corporation in the issuance of X.509 Public Key Certificate credentials to entities that will be residing inside EMC or that have a need to connect to EMC.

EMC Corporation's ESRS2CA issues certificates to members of the ESRS infrastructure to establish verified and authenticated sessions into EMC's network environment. This includes gateways, hosts, and telecom devices that reside inside and outside of EMC.

General Provisions

Disclaimers of Warranties and Obligations

Although EMC Corporation makes its best efforts to ensure that correct credentials are issued only to appropriate members of the ESRS community, EMC Corporation has no actual control over how members of the community protect their own credentials. UNDER NO CIRCUMSTANCES IS EMC CORPORATION RESPONSIBLE FOR THE CONSEQUENCES TO A RELYING PARTY OF MAKING USE OF CREDENTIALS EMC ISSUES. EMC OFFERS NO WARRANTY OF ANY KIND AND DISCLAIMS ANY WARRANTY OF MERCHANTABILITY OR OF FITNESS FOR A PARTICULAR PURPOSE. EMC CANNOT BE HELD LIABLE FOR ANY DAMAGES OF ANY KIND WHETHER DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL EVEN IF EMC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Subscriber Obligations

Subscriber shall only use this certificate where required by EMC for authentication and identification purposes. Subscriber shall not transfer this to other systems or users. Subscriber shall notify EMC via established business channels if the integrity of the certificate is compromised.

Publication and Repository

The Certificate Practice Statement (CPS) has been approved by the EMC Office of Information Security, which is part of the Global Security Organization.

Liability, Fees & Financial responsibility

Not applicable to this internal EMC ESRS2CA.

Compliance audit

An EMC internal compliance audit is periodically performed by EMC's Office of Information Security, which is part of the Global Security Organization.

Operational Requirements

Authentication Upon Registration

EMC verifies the identity of the subscriber via the ESRS portal application where the application enforces the appropriate authentication depending on the user type as well as the origin of the request. Only authenticated and authorized ESRS portal users can enroll and obtain a certificate issued by ESRS2CA.

The possession of a certificate issued by this ESRS2CA implies that at some point EMC believed that the possessor or target entity was a member of ESRS community. However the mere possession of a certificate should not be construed by relying parties that the possessor has a current association with EMC or that possession may legally bind EMC in any form of negotiation.

Need for Names to Be Meaningful

The DN field of the certificate request should be descriptive enough to identify ESRS community members.

Uniqueness of Names

Each certificate request must have a unique DN, which should be derived from the customer name, site ID and MAC or network properties of the requesting system.

Lifetime of Issued Credential

Certificates issued by this ESRS2CA are valid for no more than 25 years from the date of issuance.

Revocation

This ESRS2CA revokes certificates via a Certificate Revocation List. EMC will revoke a certificate when informed by the certificate owner or by the ESRS process that the key associated with the certificate may have been compromised or ESRS participation has been terminated.

EMC ESRS gateways (CSS) will check this url as part of the session authentication process. This url is also embedded in the CA certificate attribute <CRL Distribution Point>.

End-User Private Key Protection

EMC requires that the private keys are to be password protected while stored in the local system drives. The security of such stored files will depend on the security of the distributed file system and the

strength of the password/key chosen by the installer or the program to protect the stored file.

Certificate Profiles and Attributes for ESRS2CA

CA Certificate Profile

Certificate Authority: ESRS2CA

Nickname: ESRS2CA

Default Jurisdiction: ESRS2CA

Certificate Chain: Self-signed

Issuing Jurisdiction ID: d8b8f9e352728c50da4d8c8e73a638a895d034e3

Issuing Jurisdiction Name: ESRS2CA

Status: Active

Certificate ID (MD5): 08c77c790584965542872df468286b89

Serial No.: 96FBD245B9C7E0209B5285EB32F8A84F

Subject DN

Common Name (CN): ESRS2CA

Organizational Unit (OU): Global Security Organization

Organization (O): EMC Corporation

Country (C): US

Valid From: Friday, October 30, 2009 12:32:59 PM

Valid Until: Saturday, October 28, 2034 11:31:00 AM

Certificate (PEM format): Fingerprint:90a1ed9aa52e08c7a3215b24b3bf9b26

Signature Algorithm: rsaEncryption

Digest Algorithm: SHA1

Key Size: 2048 bits

Client Certificate Attributes

SSL Server

SSL Client

Types: CN,O,OU,SN,EA,PSEUDO,UNSTRUCTUREDADDRESS

Labels: <Common Name>,<Organization>,<Organizational Unit>,<Client Serial Number>,<E-mail Address>,<Pseudonym>,<Unstructured Address>

Default Values: <>,<>,<>,<>,<>,<>,<>

IncludeInCertDN

Flags: 1,1,1,1,1,1,1

IncludeInSDA Flags: 0,0,0,0,0,0,0

IncludeInSAN Flags: 0,0,0,0,0,0,0

Hide Flags: 0,0,0,0,0,0,0

Editable Flags: 1,1,1,1,1,1,1

Required Flags: 0,0,0,0,0,0,0

Enforce DN Definition: Disabled

Directory String

Encoding: PRINTABLE_WITH_UTF8_STRING

CRL Distribution Points

Choice: URI

Location: http://esrs-crl.emc.com/ESRS2CA.crl

A Certificate Revocation List file is generated daily. This file has a validity period of seven days.

Key Recovery

Key Recovery: Disabled

Security audit procedures

Types of event recorded

All significant security events on ESRS2CA software are automatically time

stamped and recorded in audit trail files. These include but are not limited to the following events:

- Successful and failed attempts to create, remove, login as, set reset and change passwords of and revoke privileges of ESRS2CA operative personnel and its Registration Officer;
- Failed interactions with the directory including failed connection attempts, read and write operations by ESRS2CA software; and
- All events related to certificate revocation, security policy modification and validation, ESRS2CA software start-up and stop, database backup, cross certification, attribute certificate management, DN change, database and audit trail management, certificate life-cycle management and other miscellaneous events.

Frequency of processing log

Critical system events, access attempts and CA operation events are logged on a daily basis. The audit trail is reviewed once a year.

Retention period for audit log

The monthly backup of the audit trails files are retained for ten (5) years under normal operations.

Physical, Procedural and Personnel Security

Site Location, Construction and Physical Access

The CA is located in a data enter facility with badge access. In addition, the CA is locked in a security cabinet.

Trusted Roles

The CA is managed and administered by EMC's Global Security Office (GSO) engineering security officers and operational security engineers.

Background, Qualifications, Experience, and Clearance

Requirements

All members of the Global Security team, including existing employees, potential new hires, or transferred employees will have periodic background investigations conducted in accordance with standard EMC corporate background investigations procedures. Due to the sensitive nature of system and data accessible to members of the Global Information Security Team, updates will be conducted every two years after the initial investigation.

EMC's Public Key Infrastructure is designed, deployed and maintained by qualified security professionals.

Technical Security Controls

Public Key Delivery to Certificate Issuer

The Certificate is delivered to the subscriber via on-line as described in [RFC2510].

Network Security Controls

The CA and RA are protected by layer-3 filtering firewalls and only SSL protocol is allowed for subscribers to the RA.

CA Private Key Protection

The private key for this ESRS2CA is maintained in a FIPS-140 Level-3 tamper-proof hardware.

Only designated security officers with operator smart cards have direct access to this key. EMC can make no representation of the strength of that hardware protection. No assurance beyond that provided by the manufacturer, nCipher, can be provided.

Life-Cycle Security Assurance

The CA and RA software are periodically updated and patched as per RSA Keon product guideline.

Compromise and Disaster Recovery

EMC has a comprehensive business continuity plan to enable complete recovery of all CA systems in the event of a disaster.

Contact Details

Questions about this Certificate Policy or Certification Practices Statement should be directed to GSO at EMC (pkiadmin@emc.com).

4

ESRS Security FAQ

This chapter provides answers to frequently asked questions about EMC Secure Remote Support security.

The chapter includes the following sections:

- Certificates and Encryption 32
- Communications 35
- Policy Manager 36
- Remote management 37
- Customer environment 38
- Testing 39

Certificates and Encryption

Is the connection from the ESRS gateway to EMC mutual SSL authentication?

Yes

How does the Certificate enrollment work?

During the site ESRS Client installation, digital certificates are installed on the ESRS Client. This procedure can only be performed by EMC Global Services professionals using EMC-issued RSA SecurID Authenticators. All certificate usage is protected by unique password encryption. Any message received by the ESRS Client, whether pre- or post-registration, requires entity-validation authentication.

Digital Certificate Management automates the ESRS Client digital certificate enrollment by taking advantage of EMC's existing network authentication systems, which use the RSA SecurID Authenticator and the EMC local certificate authority (CA). Working with EMC systems and data sources, Digital Certificate Management aids in programmatically generating and authenticating each certificate request, as well as issuing and installing each certificate on the ESRS Client.

ESRS Digital Certificate Management provides proof-of-identity of your ESRS Client. This digital document binds the identity of the ESRS Client to a key pair that can be used to encrypt and authenticate communication back to EMC. Because of its role in creating these certificates, the EMC certificate authority is the central repository for the EMC Secure Remote Support key infrastructure.

Before the CA issues a certificate requested for an ESRS Client the CA performs full authentication of a certificate requester using EMC-issued RSA SecurID Authenticator and verifies that the EMC Global Services professional making the request has been authenticated, and belongs to the EMC Global Services group that is allowed to request a certificate for the customer's ESRS Client. The CA then verifies that the information contained in the certificate request is accurate, and for the customer site at which the ESRS Client certificate is to be installed.

The EMC Global Services professional requests a certificate by first authenticating himself or herself using an EMC-issued RSA SecurID Authenticator. Once authentication is complete, the ESRS Client Installation (DCM) program locally gathers all the information required for requesting certificates and generates the certificate request, a private key, and a random password for the private key. The ESRS Client installation (DCM) program then writes the certificate request information to a request file, ensuring accuracy and completeness of the information.

The installation (DCM) program then submits the request to the CA over an SSL tunnel. After the Certificate request is verified, a certificate is issued and returned over the SSL tunnel. The installation (DCM) program then automatically completes the certificate and keys installation on the ESRS Client.

Note: Due to EMC's use of RSA Lockbox technology, a certificate cannot be copied and used on another machine.

Self-signed certificates take away the trusted authentication mechanism that verification by a trusted third party provides

The ESRS Gateway Client Certificate is issued by EMC Certificate Authority ESRS2CA. This Certificate Authority (CA) functions as a standalone CA and is not chained to any commercially trusted public CA. Please refer to Chapter 3, "ESRS Certificate Policy,".

Is there any type of finger print check carried out on the certificate?

Yes, during the TLS client-authenticated TLS handshake.

Can a certificate be authenticated as being from a certain device and if so how?

The certificates on each ESRS gateway are unique

What is the Certificate life cycle?

25 years

Can the key life be specified?

No, key life is fixed. However, provisioning a new gateway will create a new key.

If a key is compromised what is the revocation procedure?

Contact EMC immediate to revoke the client certificate. ESRS2CA Certificate Authority revokes certificates via a Certificate Revocation List.

What is the RSA token used for?

Only EMC authorized ESRS users authenticated with RSA token can enroll and obtain a certificate issued by EMC ESRS2CA Certificate Authority for an ESRS Client.

Are the keys generated added to an EMC key store (web of trust)?

Use of self signed Certificates on Policy Manager Web interface will produce an error message every time users access this website. That is true for the default certificate. Parameters of the certificate can be changed. Or the Customer may install a certificate of the own for use by the Policy Manager. The Process and procedures for doing this are explained in detail in the *EMC Secure Remote Support Policy Manager Operations Guide* located on EMC Powerlink at Home > Support > Technical Documentation and Advisories > Software ~ S ~ Documentation > Secure Remote Support > Secure Remote Support (ESRS 2) > Maintenance/Administration.

CAUTION

Changing the security parameters of the Policy Manager are the customers responsibility and should NOT be performed by EMC Global Services professionals.

Note: The variable HostName is the fully qualified name of the Policy Manager host system.

For additional information about SSL certificates (an Identity Keystore File) for Apache Tomcat, refer to the following website:

http://tomcat.apache.org/tomcat-5.5-doc/ssl-howto.html

Communications

What data is sent from the customer to EMC?

Configuration information: Yes

Debugging information: Yes

Passwords: No

Can information be sanitized before being sent? Not automatically

Can data be inspected before being transmitted? Not automatically

Is the connection from the External gateway to the device a new tunnel, or does it route straight through to the end device?

Communications from EMC to a supported devices is routed through the ESRS Client. EMC Support Personnel connect through the ESRS Client **not** to the ESRS Client.

Does the traffic that is being sent over the internal network need to be encrypted.

Most remote support applications used by EMC Support Personnel employ some form of encryption (SSL; HTTTPS, SSH, etc) and this cannot be changed.

Does the XML and SOAP conform to industry standards, and is the specification published?

The specification is not published. The customer cannot monitor the outgoing data.

What data can an EMC support person see on the customer device? Can the blocks be copied?

This is device dependent and is explained in the following document:

http://powerlink.emc.com/km/live1/en_US/Offering_Technical/Technical_Documentation/300-006-083.pdf

Ask your local EMC Global Services professional for the latest version.

Packet sizes of Heart beat packets?

5-10kb

What ports and protocols will ESRS use?

The EMC devices and their respective port numbers and protocols are listed in *Secure Remote Support Port Requirement* located on EMC Powerlink at Documentation and Advisories > Software ~ S ~ Documentation > Secure Remote Support > Secure Remote Support (ESRS 2) > Installation/Configuration.

Policy Manager

Who is supporting this application?

The customer will manage the ESRS client and Policy Manager on behalf of the customer. Patches/updates are supplied by EMC.

What version of Apache Tomcat is the Policy Manager running?

Version 5

What version of the HSQLDB is the Policy Manager running?

1.8.0.10

Will Patching of the Policy Manager cover issues surrounding Tomcat and HSQLDB?

Yes if necessary

Will EMC notify of vulnerabilities in Tomcat and HSQLDB?

Yes

Why can the logging be recorded on a remote machine?

Policy Manager can Syslog audit/logging information to an external Syslog server. Customer manages this using Log Logic servers.

Remote management

What remote software is installed?

Refer to the *EMC Secure Remote Support Site Planning Guide* located on EMC Powerlink at Home > Support > Technical Documentation and Advisories > Software ~ S ~ Documentation > Secure Remote Support > Secure Remote Support (ESRS 2) > Installation/Configuration

Solution can provide up to twenty concurrent connections how are they to be managed?

Policy Manager – Customer will create a process once ESRS is installed and they are familiar with the application.

Termination of sessions?

Yes, via the Policy Manager

Tracking of EMC users on line?

Yes, EMC employee ID is part of the audit record on the Policy Manager.

Can the Policy Manager / ESRS Client terminate remote support sessions if they have been inactive for a period of time?

Not automatically

Can a customer's support person shadow the session?

No, as the Support Applications are run in client/server mode.

Customer environment

Is the ESRS client running as a system service level within the OS?

Yes, however this can be changed to use locally-created service accounts for the following services:

Note: These accounts should be configured with passwords that do not expire:

- ESRS Policy Manager
- ESRS Gateway Client
- ESRS HTTPS Listener
- ESRS Watchdog

Where are details for patch management (OS and application) and methods to monitor vendor notification?

Hardware and OS patched and managed by the customer. The ESRS client application will be managed by EMC support personnel.

Policy Manager communicates to ESRS gateway over HTTP port 8090. What is this used for and can it be done over SSL?

It can be HTTP port 8090 or HTTPS SSL port 8443. HTTPS SSL is preferred. Generally defined at time of install but can be implemented post install. Process and procedures are available in the *EMC Secure Remote Support Policy Manager Operations Guide* located on EMC Powerlink at Home > Support > Technical Documentation

and Advisories > Software ~ S ~ Documentation > Secure Remote Support > Secure Remote Support (ESRS 2) > Maintenance/Administration.

Can the ESRS be locked down to only communicate with specific EMC IP addresses?

Yes, through the customer firewall rules.

Testing

Is documentation available to describe the ESRS test environment and the belief in testing in a live environment?

The possibility of live data being used for testing is against some customer standards. Documentation is available to reflect the desired ESRS test environment. Contact your EMC representative.