

# Security in EMC CentraStar 4.0

## *A Detailed Review*

---

### **Abstract**

This white paper is an introduction to the security architecture, measures, and practices of the 4.x releases of the CentraStar<sup>®</sup> server and the EMC<sup>®</sup> Centera<sup>®</sup> SDK. Topics discussed are network security, access security, data security and protection, and service-related security procedures.

July 2008

---

---

Copyright © 2008 EMC Corporation. All rights reserved.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS IS.” EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on [EMC.com](http://EMC.com)

All other trademarks used herein are the property of their respective owners.

Part Number H4495

---

## Table of Contents

<b>Executive summary .....</b>	<b>5</b>
<b>Introduction .....</b>	<b>5</b>
Audience .....	5
<b>What is new in CentraStar 4.0?.....</b>	<b>5</b>
Message of the Day .....	5
Password complexity rules .....	5
<b>What is new in CentraStar 3.1.3?.....</b>	<b>6</b>
TLS/SSL support.....	6
X.509 certificates .....	6
Password protection .....	7
Challenge-response authentication .....	8
IP restrictions .....	8
<b>CentraStar security principles .....</b>	<b>8</b>
Authentication .....	8
Access profile .....	9
Profile secret.....	10
PEA file.....	11
CLI/CV login .....	11
Connection string .....	11
Authorization .....	12
Virtual pool.....	13
Capability.....	14
Role .....	15
Home pool .....	15
Access profile Access Control List .....	16
Cluster pool and cluster profile.....	16
Auditing .....	17
Audit information storage .....	17
Viewing audit information .....	17
Access.....	17
Application server access.....	17
Management and service access.....	18
Locking a cluster .....	18
Remote Management Access on CE+ clusters .....	18
Management IP Restriction .....	19
Replication and restore connections .....	19
<b>Service security .....</b>	<b>19</b>
EMC Centera Viewer and EMC Centera Command Line Interface.....	19
Connect home using SMTP .....	20
SNMP .....	20
MoPI.....	20
Dial-in support.....	20
Controlled and audited platform access with sudo .....	21
OnAlert .....	21
Connect home using OnAlert .....	21
Dial-In using OnAlert .....	21

---

EMC Secure Remote Support Gateway .....	22
Offsite EMC personnel connecting to EMC to provide customer support .....	23
Data protection.....	23
<b>Conclusion .....</b>	<b>23</b>
<b>References .....</b>	<b>23</b>

---

## Executive summary

EMC Centera<sup>®</sup> is the world's most simple, affordable, and secure repository for information archiving. EMC Centera greatly simplifies the task of managing, sharing, and protecting all sizes of content repositories. Information is protected at an object level. EMC Centera safeguards access through the use of authentication/authorization, access profiles, management profiles, system logging and auditing, and virtual pools. The archiving platform enforces retention and disposition intrinsically in storage while addressing business continuity and disaster recovery.

## Introduction

This white paper is an introduction to the security architecture, measures, and practices of the 4.x releases of the CentraStar<sup>®</sup> server and the EMC<sup>®</sup> Centera<sup>®</sup> SDK. This paper covers the following topics:

- What is new in CentraStar 4.0
- What is new in CentraStar 3.1.3
- CentraStar security
  - Authentication
  - Authorization
  - Auditing
- Service

## Audience

This white paper is intended for customers, including storage architects and administrators and any others involved in evaluating, acquiring, managing, operating, or designing an EMC Centera storage environment. It is also intended for EMC staff and partners for guidance and development of proposals.

## What is new in CentraStar 4.0?

### *Message of the Day*

On the server, a separate Message of the Day (MOTD) for customers and for EMC users can be stored in cluster parameters. CLI commands are provided to show and edit these. The MOTD will be shown after connecting with CV, stand-alone CLI, and ssh. EMC users will see both the customer MOTD and the EMC MOTD. Customers will not see the EMC MOTD.

### *Password complexity rules*

CLI functionality for managing password complexity on all passwords that are set when creating or updating profiles has been introduced. In the CLI, the commands “set password rules” and “show password rules” change and show the currently set [password policy](#). The following rules are implemented:

- Setting the minimum password length (FIPS standards state the use of at least eight characters)
- Ability to prohibit passwords with all alphabetic or all numeric characters
- Ability to prohibit passwords with consecutive identical characters
- Ability to force the use of special characters such as @, #, \$, %, & in the password
- Ability to force the use of both lowercase and uppercase characters

---

## What is new in CentraStar 3.1.3?

### ***TLS/SSL support***

With CentraStar 3.1.3, TLS/SSL encrypted connections are used for all management connections. TLS is the successor of SSL, and is backwards compatible with SSL 3.0. Using TLS for all management connections ensures that data exchanged between management clients and EMC Centera cannot be corrupted without detection, and allows system administrators to check whether they are connected to the right EMC Centera. TLS operation requires an X.509 server certificate on EMC Centera. A new or upgraded EMC Centera will be configured with a self-signed certificate initially, and can be updated to use a certificate from a [Certificate Authority](#) (CA) if desired. The supported certificate formats are [PEM](#), [DER](#), [PKCS#12](#).

SSL/TLS and X.509 certificates are well suited for Internet communications, where a customer does not have complete control over the environment. In corporate data centers, the default self-signed certificate generated by EMC Centera will usually be sufficient. Customers can use external tools to generate their own certificate, or to obtain a certificate from a CA.

### ***X.509 certificates***

X.509 certificates are analogous to a passport. A certificate provides proof that a [public key](#) belongs to a specific system or person. Certificates can be obtained from a Certificate Authority (CA), generated by [external CA tools](#), or generated by the EMC Centera internally (this is done by default). A CA is like the passport office, which verifies your identification and creates a trusted document that certifies who you are and issues the document to you. The certificate a CA provides to identify the customer (or their systems) is referred to as the server certificate. The certificate of a CA is called a [root certificate](#).

A self-signed certificate is generated by default during a new install or upgrade by EMC Centera. This self-signed certificate is valid for 3 years. In this instance EMC Centera is acting as its own CA. This proof of authenticity is considered strong enough for use of EMC Centera within a data center. The ability to generate a self-signed certificate makes sure that EMC Centera management links can always be encrypted.

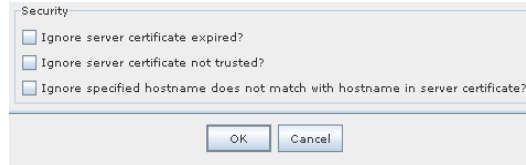
Customers requiring stronger proof of authenticity can install their own certificate. Customers can generate their own certificate with external tools, or obtain one from a CA. When using externally generated server certificates, the root certificate of the CA used to generate the server certificate needs to be installed on the client systems to verify the trust chain.

**Table 1. New CLI commands for certificate support on EMC Centera**

<b>set certificate</b>	Installs a new certificate chain.
<b>show certificate</b>	Shows the currently installed certificate chain.
<b>delete certificate</b>	Deletes the current certificate chain and replaces it with a new self-signed certificate.

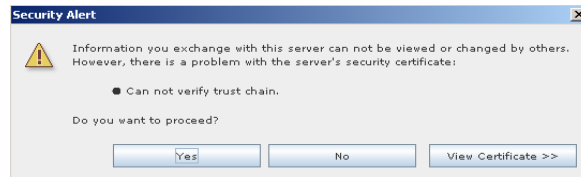
“set certificate” supports the following formats: PEM, DER, PKCS#12. When using “set certificate”, the validity will be checked. Certificates that have expired and certificates with a validity date over 10 years will be rejected.

In the updated management tools (CentraViewer, CLI, and so on) certificate expiration, trust chain, and hostname are all validated, and can produce error/warning messages. These checks can be configured from the CV preferences.



**Figure 1. Centera Viewer security preferences**

When CV/CLI connects to EMC Centera for the first time, or when a server’s certificate is updated, the following dialog box will be displayed:



**Figure 2. Centera Viewer/CLI Security Alert**

You can click Yes to continue using the application while not trusting the certificate, No to not trust the certificate and not connect to the server, or View Certificate >> to show the information about the certificate and allow it to be installed on the client. If you click View Certificate >>, you will be given the choice to install the root certificate, or server certificate.

In Centera CV you can install either a server certificate or a root certificate, also known as the public certificate of the CA the customer trusts. This root certificate is used to verify the certificates of the EMC Centera to which you are connected, and should be installed when you use a server certificate that is externally generated.

When an X.509 certificate expires, it will remain installed on EMC Centera. The EMC Centera system administrator must either install a new certificate, or use the “delete certificate” command to generate a new certificate. CV will notify you when a server certificate is expired, unless you selected the Ignore server certificate expired? setting.

A potential configuration problem is that only one certificate can be installed on a system, while there are several access nodes that a management connection can use. To avoid this problem, either the DNS entry for the hostname in the certificate should refer to all IP addresses of the access nodes, or the server certificate should use a wildcard (for example, \*.centera.emc.com).

## ***Password protection***

Formerly all passwords were stored on EMC Centera in base64 encoded form. Now there are two schemes for password persistency:

<b>hashed</b>	For EMC Centera management connections only
<b>obfuscated</b>	For EMC Centera profiles that use challenge-response authentication (SDK and old management clients)

Profiles that require challenge-response authentication cannot use the hashed password protection scheme. The management client software (CV, CLI) version 3.1.3 is required to use hashed password protection. To enable data access for a profile, the obfuscated format is required. Profiles can be updated to change the password persistency scheme in the CLI or CV. A warning is given when a profile is changed from obfuscated to hashed format. Only profiles with the AccessControl management role can change the password persistency scheme for a profile. On upgrade, all base64 encoded passwords will automatically be converted to the obfuscated format. PEA file and profile export functions will not be affected.

---

## Challenge-response authentication

The challenge-response authentication algorithm has been updated from HMAC-MD5 to HMAC-SHA256. Centra SDK version 3.2 or later is required to use the newer algorithm. Older applications that use the previous algorithm (HMAC-MD5) can still connect without problem to CentraStar 3.1.3 clusters.

## IP restrictions

In EMC Centra 3.1.3, the Management IP Restriction feature has been updated. Now restrictions can be configured per profile for both SDK and management connections. A list of IP addresses can be associated with each profile. When a profile has a list of restricted IP addresses, connections with this profile are only allowed from any of these IP addresses. Customers using previous IP Restrictions features need to manually reconfigure using the new enhanced feature after upgrading to 3.1.3. New CLI commands to support the Management IP Restriction per profile are:

<b>show ip restrictions</b>	Provides a list of all profiles with the IP restrictions
<b>update ip restrictions 'profile name'</b>	Allows adding or removing of IP restrictions

There are no restrictions enabled by default. Restrictions can be added or removed with the “update ip restrictions ‘profile name’” command. Restrictions can be shown for all profiles by using the “show ip restrictions” command, or individually with the “show profile detail” command in the CLI. Additionally, the system health report will show whether restrictions exist or not (the IP addresses are not shown for security reasons), and the CCC report will show all IP restrictions.

## CentraStar security principles

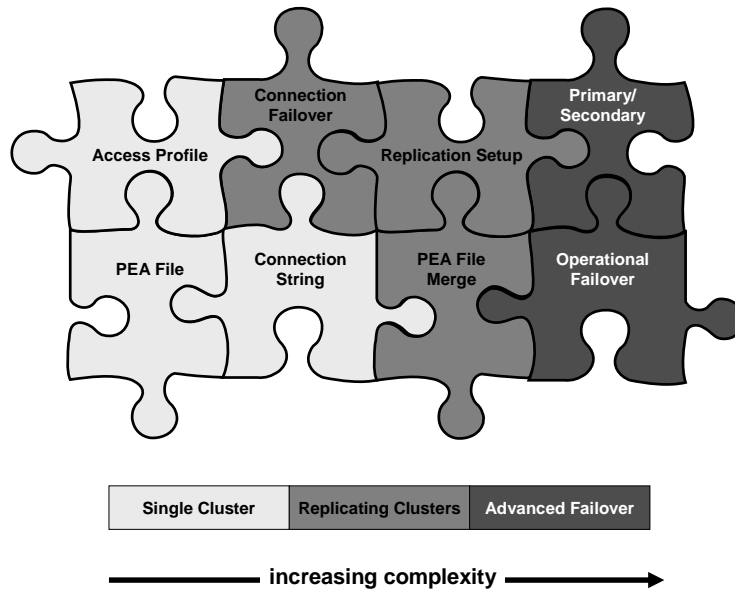
### Authentication

Authentication is the process of verifying a CentraStar user’s identity. CentraStar uses a challenge-response application authentication approach based on RFC 2104 HMAC<sup>1</sup>. As of CentraStar 3.1.3, the challenge-response authentication algorithm has been updated from HMAC-MD5 to HMAC-SHA256. Centra SDK version 3.2 or later is required to use the newer algorithm. Older applications, which use the previous algorithm (HMAC-MD5), can still connect without problem to clusters running CentraStar 3.1.3 (and later).

An application (through the Centra SDK), or a management user (through management tools like CLI/CV), pass authentication information into an authentication module. The authentication module implements all the functions to handle the transfer of the authentication information and the challenge/response interactions. When a cluster receives an authentication request, it generates a challenge. The challenge is a random number used for that single connection. The connecting application uses a cryptographic formula that accepts the access profile secret and the challenge as input parameters and generates the response. The cryptographic formula has the following properties: the response can only be computed if the secret is known and it is impossible to derive the secret from the response. The response is sent back to the cluster, which also generates the response and compares it with the response received from the connecting application or management tool.

---

<sup>1</sup> More information on Hashed Message Authentication Codes can be found at: <http://www.ietf.org/rfc/rfc2104.txt>



**Figure 3. Assembling authentication building blocks**

The following sections will familiarize you with the various authentication concepts, from the most basic to the more advanced.

## Access profile

Access profiles<sup>2</sup> are used by access applications and management tools to authenticate to a cluster, and by clusters to authenticate themselves to each other for replication or restore connections. They are created on the cluster using the EMC Centra Command Line Interface (CLI) using the “create profile <profilename>” or “update profile <profilename>” commands.

There are three types of access profiles:

### Application profiles

Application profiles are a means to enforce<sup>3</sup> authentication and authorization for applications that access a Centra through the Access API. The administrator can determine which applications have access to which pool and what operations they can perform on the pool data by assigning a set of capabilities. Each application profile has a default home pool assigned to it; the home pool is the only pool where the profile can create new C-Clips.

### Cluster profiles

Cluster profiles differ from regular application profiles in the following ways:

- The home pool of a cluster profile is the cluster pool.
- An application that is using a cluster profile cannot perform normal writes. This means that new C-Clips cannot be created. However, a cluster profile can use the clip-copy functions to restore existing C-Clips from replica clusters or external media.
- If the cluster pool grants a capability to a cluster profile, the application using this cluster profile will be able to delete any C-Clip regardless of the pool in which it resides, or the pool Access Control List and mask.

<sup>2</sup> Since CentraStar 3.0, the Root Profile has been removed and replaced with the Cluster Mask. The section “Authorization” or the Centra Online Help provides more information.

<sup>3</sup> EMC recommends customers not use the Anonymous profile, which allows applications to connect without authentication. As of CentraStar 3.1, the Anonymous Profile is disabled by default. It is still supported for backwards compatibility.

- Cluster profiles are intended to be used by backup/restore style operations.

### Management profiles

Management profiles are used by system administrators and EMC Service personnel to authenticate to EMC Centra when using management tools such as CV and CLI. The system administrator can create management profiles and assign one or more predefined manageability roles (The section “Authorization” provides more information) that determine which actions the user of the management profile is allowed to perform on the EMC Centra cluster.

System administrators can use one of the two built-in management profiles to log in to CV or the CLI: admin and console. Table 2 shows the manageability roles, capabilities, home pool, and secret for these profiles.

**Table 2. Profiles**

Profile	Admin	Console
<b>Roles</b>	accesscontrol, audit, compliance, configuration, monitor, replication	Monitor
<b>Capabilities</b>	-	rdq--cw---
<b>Home pool</b>	Default	ConsoleArchive
<b>Secret</b>	centera	Console

It is recommended to limit the use of the admin profile and use custom management profiles instead. If the admin password is lost, only EMC Service can reset it. EMC Service engineers have their own set of profiles to perform service actions on EMC Centra. The system administrator cannot change the roles or secret of the EMC Service profiles.

Management profile users are allowed and encouraged to change their password using the CLI using the "set security password" command.

### Profile secret

The secret, or password, is the most important parameter that must be provided for an access profile, other than its name. The system administrator has the following options<sup>4</sup> available:

- **Generated:** Strong secrets are automatically generated by CentraStar (default).
- **File:** The system administrator can provide the path to a file containing a non-encoded, human-readable secret.
- **Prompt:** The system administrator can also type in a non-encoded, human-readable password using the prompt option (since CentraStar 3.1). A popup will appear to type the secret.

Prior to CentraStar 3.1.3 all passwords were stored on EMC Centra in base64 encoded form. As of CentraStar 3.1.1 there are two schemes for password persistency:

hashed	Used for EMC Centra management connections only
obfuscated	Used for EMC Centra profiles that use challenge-response authentication (SDK and old management clients)

Profiles that require challenge-response authentication cannot use the hashed password protection scheme. Management client software (CV, CLI) version 3.1.3 or later is required to use hashed password protection. To enable data access for a profile, the obfuscated format is required. Profiles can be updated to change the password persistency scheme in the CLI or CV. A warning is given when a profile is changed from obfuscated to hashed format. Only profiles with the AccessControl management role can change the

<sup>4</sup> When the Access Profile is to be used by management users, the profile secret must be human-readable and only the <file> or <prompt> options should be used.

---

password persistency scheme for a profile. On upgrade, all base64 encoded passwords will automatically be converted to the obfuscated format. PEA file and profile export functions are not affected.

## PEA file

A Pool Entry Authorization (PEA) file, generated using either the CLI “create profile <profilename>” or “update profile <profilename>” command, is a clear text, XML formatted, non-encrypted file that can be used by system administrators to communicate and distribute authentication credentials to application administrators.

A PEA file is optional for access profiles with secrets that were defined using the prompt or file option but it is necessary for using access profiles with generated secrets.

A PEA file contains the following information:

- The <defaultkey> element provides credentials that are not cluster specific. These credentials were originally designed as a fallback mechanism but are not being used in any current SDK.
- The <key> element provides a cluster-specific set of credentials that only apply for the cluster on which it was generated. The *type* tag is always set to “cluster”, the *id* tag specifies the unique ID of the cluster for which the access profile can be used, and the *name* tag displays the access profile’s name
- The <credential> elements contain the actual secret that was generated by CentraStar or typed by the system administrator for the access profile. The *id* tag is always set to “csp1.secret” and the *enc* tag is always base64.

## CLI/CV login

When using the CV or CLI, a username and password are requested. In CentraStar versions prior to 3.1, the only user available to the customer was the admin user. Since CentraStar 3.1, any access profile and associated secret can be used if they have a management role assigned.

## Connection string

The connection string is a parameter that is used by applications when they connect and authenticate to a cluster using the FPPool\_Open call in the SDK. In its most basic form, it consists of a number of IP addresses all belonging to the same cluster and credential information:

---

```
ADDRESS := [primary=]ip_address|domain_name
ADDRESS_LIST := ADDRESS[,ADDRESS_LIST]
CREDENTIAL := [[path=]file_system_path|name=Access Profile_name|secret=Access Profile_secret]
CREDENTIALS := CREDENTIAL[,CREDENTIALS]
CONNECTION_STRING := ADDRESS_LIST[?CREDENTIALS][,CONNECTION_STRING]
```

---

### Figure 4. Connection string format

EMC recommends specifying the IP addresses of at least two of the access nodes for each cluster to which the application wishes to connect. This ensures that a connection can be made even if one of the access nodes is offline. You can specify more access nodes (or all of them) for all the clusters you will connect to with the application in the connection string; this will ensure a connection can be made even if one or more of the access nodes are offline (as long as one is still online).

The SDK will probe and attempt<sup>5</sup> a connection to each address specified in the connection string. After each successful connection, which is still unauthenticated at this point, the cluster communicates the full list of access nodes to the SDK. The IP addresses of these nodes are added to the list of connection addresses and they too are probed. Failing to establish a connection to one or more addresses does not prevent establishing the pool connection as long as one connection can be made. The SDK will then attempt to authenticate the application using a set of credentials in the form of an access profile name and

---

<sup>5</sup> The SDK will retry a connection a number of times; the number of retries can be set by the application administrator; the *EMC Centra SDK Programmer’s Guide* provides more information.

secret. EMC Centera offers three options to provide authentication credentials, listed below in order of priority<sup>6</sup>:

- The first credentials checked are those provided in the form of an access profile name and password<sup>7</sup> in the connection string.

```
FPPool_Open("primary=10.2.3.4,primary=10.6.7.8?name=Access Profile_name,secret=Access Profile_secret")
```

- The second set of credentials checked are those provided as a path<sup>8</sup> to a PEA file (generated on the cluster and stored on the application server) in the connection string.

```
FPPool_Open("primary=10.2.3.4,primary=10.6.7.8?path=c:\Access Profile.pea")
```

- The third option for providing credentials uses a system environment variable on the application server called `CENTERA_PEA_LOCATION`. The content of the `CENTERA_PEA_LOCATION` can again be defined as either (1) a path to a PEA file or (2) the actual authentication credentials.

- `CENTERA_PEA_LOCATION == path=c:\Access Profile.pea`
- `CENTERA_PEA_LOCATION == name=Access Profile_name,secret=Access Profile_secret`  

```
FPPool_Open("primary=10.2.3.4,primary=10.6.7.8")
```

In order to determine which option is best for your specific use case, consult Table 3.

**Table 3. Weighing authentication options**

	Access profile name/password	PEA file
Connection String	Least amount of effort to set up	Supports strong encoded secrets Access profile and secret can be different on replicating clusters
Environment Variable	Supports applications that do not allow access to connection string	Supports applications that do not allow access to connection string Supports strong encoded secrets Access profile and secret can be different on replicating clusters

If no authentication credentials can be found at all, the application will request access with the anonymous profile.

---

NOTE: EMC highly recommends the system administrator to disable the anonymous profile on a cluster, thereby denying access without a properly defined access profile.

---

## Authorization

Authorization is the concept of allowing access to resources only to those permitted to use them. An application or management tool that has successfully authenticated with a cluster (using an access profile name and secret) is allowed access to cluster resources based on the access capabilities and management roles assigned to the access profile. The same applies to the replication and restore processes, which also use an access profile to connect to a replica or target cluster. Again, replication and restore will be granted a number of capabilities on all or parts of the content of the cluster.

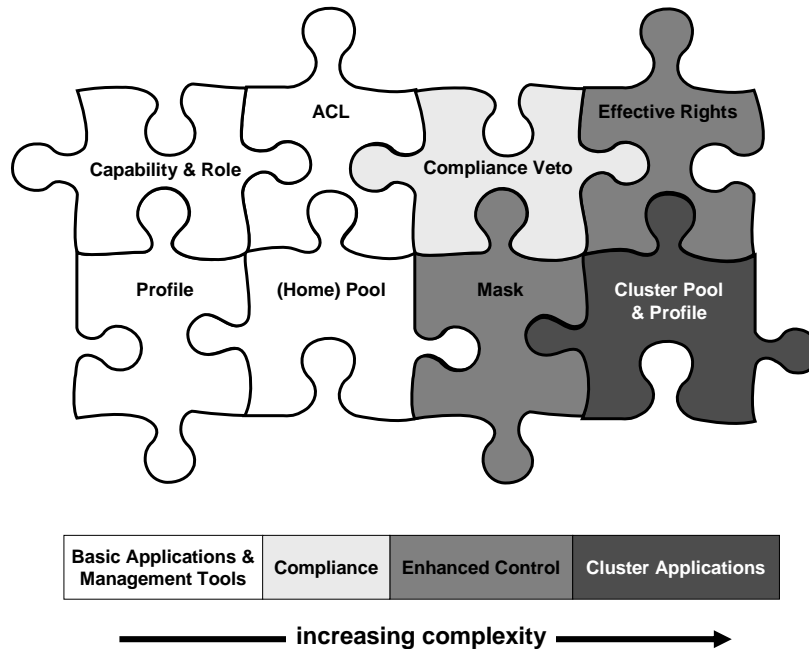
The following section will familiarize you with EMC Centera authorization concepts.

---

<sup>6</sup> Conflicting credentials are parsed in the following priority: (1) specific credentials using `name=` and `secret=` prefixes that appear in a connection string override those that are held in a PEA file; (2) `path=` credentials that appear in a PEA file override those referenced in the `CENTERA_PEA_LOCATION` environment variable.

<sup>7</sup> The profile name and secret strings are non-encoded clear text. If you selected a secret containing non-ASCII characters, you cannot use this option.

<sup>8</sup> The `path=` prefix is not mandatory but it is a best practice to include it in the connection string.



**Figure 5. Assembling authorization building blocks**

## Virtual pool

Virtual pools (referred to as pools in the remainder of the white paper) were introduced in CentraStar 3.0 to enable system administrators to segregate data into logical groups and provide more granular access control to applications using a cluster:

- **Data Segregation:** C-Clips from one application can be kept apart from C-Clips from other applications, making it possible to prevent one application from accessing C-Clips written by another application, and allowing system administrators to report on the usage of the cluster on a pool-by-pool basis.
- **Access Control:** The administrator can determine the operations an application can perform on a set of specific pools.

There are three types of pools:

- **Cluster pool:** The cluster level pool that contains every C-Clip in a cluster. There is only one cluster pool, and it cannot be deleted. It allows operations to work across the boundaries of pools when using a cluster profile.
- **Application pool:** An application level pool that typically contains data for one application. The default pool is a predefined application pool that cannot be deleted. The system administrator can create and delete custom application pools.
- **System pool:** Used to archive system information such as alert and reporting history (the ConsoleArchive pool) and audit trail information (the AuditArchive pool).

Every C-Clip in the cluster belongs to exactly two pools: the cluster pool and one application or system pool. All C-Clips are members of the cluster pool by definition.

Note that the cluster pool, default pool, ConsoleArchive pool, and AuditArchive pool are built-in and cannot be deleted.

Application pools created by the system administrator are identifiable by a globally unique ID generated by CentraStar and a cluster unique display name:

- The pool ID cannot be modified.
- The pool name must be unique on a cluster.
- Pools created with the same name on different clusters will not have the same unique ID and are not the same pool. This is important for replication.

## Capability

Capabilities are rights granted by the system administrator to an access profile on a pool. These capabilities determine which SDK operations the application using the access profile can perform on C-Clips belonging to that pool. Table 4 gives an overview of the list of capabilities and the corresponding API calls that these capabilities enable.

**Table 4. CentraStar capabilities granted by pools**

Capabilities	API calls enabled	Definition
Write (w)	FPClip_Write() FPtag_BlobWrite() FPtag_BlobWritePartial() FPClip_EnableEBRWithPeriod () FPClip_EnableEBRWithClass() FPClip_TriggerEBREvent () FPClip_TriggerEBREventWithPeriod () FPClip_TriggerEBREventWithClass()	Write C-Clips. Trigger Events for Event Based Retention.
Read (r)	FPClip_Open() FPtag_BlobRead() FPtag_BlobReadPartial()	Read C-Clips.
Delete (d)	FPClip_Delete() FPClip_AuditedDelete (FP_OPTION_DEFAULT_OPTIONS)	Delete C-Clips.
Exist (e)	FPClip_Exists()	Check for the existence of C-Clips.
Privileged Delete (D)	FPClip_AuditedDelete (FP_OPTION_DELETE_PRIVILEGED)	Delete C-Clips, overruling retention periods.
Query (q)	FPPoolQuery_Open(),	Query C-Clips using a time-based query.
Clip-Copy (c)	FPClip_RawOpen() FPClip_RawRead()	Copy C-Clips; this capability is needed for replication/restore or other backup and recovery operations.
Purge (p)	--deprecated calls only--	Remove all traces of C-Clips and Blobs from the cluster; is only available for cluster profiles.
Litigation Hold (h) <sup>9</sup>	FPClip_SetRetentionHold	Set and remove litigation holds on C-Clips.

The Profile-Driven Metadata capability is not pool-aware and is granted cluster-wide to a profile.

**Table 5. CentraStar capabilities granted by the cluster**

Capabilities	API Calls Enabled	Definition
Profile-Driven Metadata (P)	--not exposed in the SDK-- --management function only--	Supports adding access profile specific metadata to C-Clips.

<sup>9</sup> In CentraStar 3.1, an application that wants to use the Litigation Hold feature also needs the write capability.

---

## Role

Roles determine what rights a management user has on the cluster after successfully authenticating. Note that an access profile can be granted both capabilities and roles. For instance, the monitor role allows applications to use the MoPI calls of the API to receive monitoring information from the cluster.

An access profile can be granted one or more of the following roles as shown in Table 6.

**Table 6. CentraStar manageability roles**

Roles	Rights
Accesscontrol	<ul style="list-style-type: none"><li>• Can configure and view profiles and pools. This includes:<ul style="list-style-type: none"><li>- Creating and changing profiles and pools</li><li>- Changing and resetting passwords for all profiles except admin</li><li>- Importing and exporting pool and profile definitions</li><li>- Granting capabilities</li><li>- Managing pool migration and capacity tasks</li></ul></li><li>• Can configure remote access security: lock/unlock nodes</li><li>• Can manage certificates</li></ul>
Audit	<ul style="list-style-type: none"><li>• Can configure audit logging settings</li><li>• Can view and download audit logs</li></ul>
Compliance	<ul style="list-style-type: none"><li>• Can configure compliance-related settings. This includes:<ul style="list-style-type: none"><li>- Retention classes</li><li>- Default retention period</li><li>- Min/max governor</li><li>- Management IP restrictions</li></ul></li></ul>
Configuration	<ul style="list-style-type: none"><li>• Can configure all settings that are not handled by the other roles. This includes:<ul style="list-style-type: none"><li>- Cluster identification and service settings</li><li>- External network configuration</li><li>- Domain configuration</li><li>- Regeneration buffer and policy settings</li><li>- SNMP and ICMP configuration</li><li>- Metadata configuration</li><li>- Power alerting</li></ul></li></ul>
Monitor	<ul style="list-style-type: none"><li>• Used for monitoring and reporting only</li><li>• Cannot change anything on the cluster</li><li>• Can subscribe to alerts and audit logs</li><li>• Can request health report</li><li>• Can issue the following MoPI calls:<ul style="list-style-type: none"><li>FPMonitor_Open</li><li>FPMonitor_Close</li><li>FPMonitor_GetDiscovery</li><li>FPMonitor_GetDiscoveryStream</li><li>FPMonitor_GetAllStatistics</li><li>FPMonitor_GetAllStatisticsStream</li><li>FPEventCallback_RegisterForAllEvents</li><li>FPEventCallback_Close</li></ul></li></ul>
Replication	<ul style="list-style-type: none"><li>• Can configure and view replication and restore. This includes:<ul style="list-style-type: none"><li>- Changing replication configuration: target cluster, pools to replicate, replication profile</li><li>- Starting restore: Target cluster, pools to restore, profile to use</li><li>- Pausing/resuming/disabling replication</li><li>- Managing Replication Parking Lots</li></ul></li></ul>

## Home pool

The home pool of an access profile is the pool in which all new data for the application using the access profile is written. An access profile has only one home pool at any point in time.

The combination of the access profile and the home pool determines the pool membership of a C-Clip.

This information is embedded in the Content Descriptor File (CDF) and cannot be changed. Hence, the membership of a single C-Clip cannot be changed explicitly.

The home pool of an access profile is assigned using the CLI “create profile” or “update profile” commands.

---

## Access profile Access Control List

The EMC Centra authorization mechanism is based on the general principle that access profiles are granted capabilities or rights on specific pools (Table 3 on page 12) or on the entire cluster (Table 4 on page 14). They are also granted certain roles for management-specific tasks.

Access profile capabilities and roles are assigned using one of three CLI commands:

- The most common is at the time of creation of a new access profile using the “create profile <profilename>” command. This command allows cluster level capabilities, and capabilities on the home pool and roles to be set.

---

Granted Rights for the Profile in the Home Pool [rdqeDcwh]:

Profile-Metadata Capability? (yes, no) [no]: Y

Accesscontrol role? (yes, no) [no]: y

Audit role? (yes, no) [no]: n

Compliance role? (yes, no) [no]: y

Configuration role? (yes, no) [no]: n

Monitor role? (yes, no) [no]: y

Replication role? (yes, no) [no]: y

---

- The same information can be specified or changed using the “update profile <profilename>” command.

---

Granted Rights for the Profile in the Home Pool [rdqeDcwh]:

Profile-Metadata Capability? (yes, no) [no]: Y

Accesscontrol role? (yes, no) [no]: y

Audit role? (yes, no) [no]: n

Compliance role? (yes, no) [no]: y

Configuration role? (yes, no) [no]: n

Monitor role? (yes, no) [no]: y

Replication role? (yes, no) [no]: y

---

- The third option is to specifically indicate that a pool grants certain capabilities to an access profile using the “set grants <pool name> <profile name>” command. This can be issued for any pool, including the home pool.

---

Granted Pool Rights for Profile [rdqeDcwh]:

---

When upgrading to CentraStar 3.0 or 3.1, existing access profiles that were created in earlier releases will automatically be associated with the default pool and retain the same capabilities for the default pool as they had on the entire pre-3.0 cluster. The monitor capability has been replaced with the monitor role.

## Cluster pool and cluster profile

An application profile is an access profile that has an application pool as its home pool. A cluster profile differs from application profiles in the following ways:

- The home pool of a cluster profile is the cluster pool.
- Cluster profiles cannot be granted capabilities on pools other than the cluster pool.
- An application that is using a cluster profile cannot perform writes. This means that new C-Clips cannot be created using a cluster profile.

The major use cases for using cluster profiles are data recovery applications, including replication and restore and CBRM, and cluster-wide processes such as Centra Seek.

---

## Auditing

With the introduction of CentraStar 3.1, the following management-related events are automatically logged:

- Every login to the system made through the CLI and CV
- Failed logins made through the Access API (using the Centera SDK)
- Every management action that has changed the configuration of the system (Console, CV, CLI, or MAPI command)
- Every management command issued on the EMC Centera platform

The information in the logs allows the system administrator to see who logged in to the system and which actions were performed when.

### Audit information storage

EMC Centera stores each log entry in:

- A C-Clip in the AuditArchive system pool for a certain period, configurable by the system administrator
- Regular log files on each node in /var (these log files are rotated frequently).

EMC Centera sends out each log entry in real time through:

- Syslog stream. Syslog is an industry-standard logging protocol using UDP port 514
- MOPI stream (for integration with EMC ControlCenter® and other MOPI applications)

### Viewing audit information

The audit log can be viewed in a number of ways:

- Through a Syslog server
- MOPI (realtime data in both structured XML and human readable format, possible to filter on start time)
- Through the CV or CLI, where an XML or tab delimited file can be downloaded for a date range

The following is an example of such an audit log:

---

```
Fri Sep 16 17:06:35 CEST 2005 [platform] Command script.sh was executed
Fri Sep 16 17:06:53 CEST 2005 [admin] Successful login for admin from 10.12.1.29
Fri Sep 16 17:07:35 CEST 2005 [admin] Pool financePool with id 640caf76-1dd2-11b2-a15d-9d8713b23f3e-10 and mask rdqeDcwpP- was created
Fri Sep 16 17:07:35 CEST 2005 [admin] The quota for pool 640caf76-1dd2-11b2-a15d-9d8713b23f3e-10 was set to 65000000000
Fri Sep 16 17:07:54 CEST 2005 [admin] The homepool of profile financeApp was changed to financePool
Fri Sep 16 17:07:54 CEST 2005 [admin] Granted profile financeApp rights rdqeDcw--- to pool financePool
```

---

**Figure 6. Audit log examples**

## Access

### Application server access

Applications communicate with an EMC Centera cluster using a set of access nodes. Access nodes are EMC Centera nodes that have been assigned the access role, have external IP addresses, and provide an

---

interface between the customer network and the cluster internal LAN. All data communication between applications and a cluster and between clusters is unencrypted.<sup>10</sup>

Introduced in CentraStar 3.1 is the ability to assign a network address translation (NAT) address to each access node in the form of a Fully Qualified Name (FQN) for communications between the application server and the cluster. This allows the actual IP address of EMC Centera to be hidden from the application administrators. Contact your service representative to enable and configure NAT.

To function properly, the following port must be opened for the trusted application servers:

**Table 7. Application server access**

Port	Direction	Service
3218/TCP	To/from Centera	TCP - SmartPacket port for data transfer
3218/UDP	To/from Centera	UDP - SmartPacket port for cluster probe

## Management and service access

The EMC Centera Command Line Interface (CLI) and Centera Viewer (CV) are tools used by the system administrator and EMC Service staff to configure and support the cluster. In some cases, EMC Service staff will need to open a shell for direct access on the EMC Centera platform. To allow these tools to connect to EMC Centera, the following ports must be opened as well:

**Table 8. Management and service access**

Port	Direction	Service
3682 TCP	To/from Centera	Remote Monitoring and Management using CLI/CV
22 TCP	To Centera	SSH daemon

## Locking a cluster

EMC strongly recommends system administrators to keep a cluster locked at all times. By locking a cluster, only the admin and other customer access profiles can make management connections to the cluster. Any current EMC Service connections (CV/CLI/SSH) will no longer be able to issue commands. Only when EMC Service needs to service the cluster should the cluster be unlocked for the duration of the service.

All nodes in a cluster are locked by default. To allow service access, the system operator can issue a “set security unlock” command in the CLI

## Remote Management Access on CE+ clusters

Prior to CentraStar 3.1, a CE+ cluster did not allow any management connections through the access nodes. With the ability to create specific access profiles for management connections and to assign specific roles to these access profiles, this restriction has been relaxed partially: When an access profile only has the monitor role, a 3.1 CE+ cluster will accept these monitoring and reporting only connections through port 3682 on access nodes.

For actual management and configuration, the system administrator must establish a temporary connection with an eth2 port on a node without the access role, and connect to the cluster in that manner. EMC also recommends connecting modems only when a remote intervention is needed.

---

<sup>10</sup> Note that authentication information is not sent over the wire—instead authentication communication uses an HMAC challenge-response protocol.

---

## Management IP Restriction

In EMC Centera 3.1.3, the Management IP Restriction feature was updated. Restrictions can be configured per profile for both SDK and management connections. A list of IP addresses can be associated with each profile. When a profile has a list of restricted IP addresses, connections with this profile are only allowed from any of these IP addresses. Customers using previous IP Restrictions features need to manually reconfigure using the new enhanced feature after upgrading to 3.1.3 or later.

New CLI commands to support the Management IP Restriction per profile are:

show ip restrictions	Provides a list of all profiles with the IP restrictions
update ip restrictions 'profile name'	Allows adding or removing of IP restrictions

There are no restrictions enabled by default. Restrictions can be added or removed with the “update ip restrictions ‘profile name’” command. Restrictions can be shown for all profiles by using the “show ip restrictions” command, or individually with the “show profile detail” command in the CLI. Additionally the system health report will show whether restrictions exist or not (the IP addresses are not shown for security reasons), and the CCC report will show all IP restrictions.

## Replication and restore connections

When multiple clusters are set up in a replication environment, the connections between them are established using the Access Nodes. For a cluster, an incoming replication connection is no different from an application server connection. The same network restrictions apply as with application connections. Note that NAT is not supported between replicated clusters.

## Service security

EMC’s reputation for outstanding system uptime and reliability is due to superior design, first-rate customer service expertise, and a proactive ability to remotely support its products. This remote support capability assumes that the customer and EMC work together to maximize EMC’s ability to anticipate potential problems and respond to prevent or correct issues. The best method to ensure this effective coordination is for the EMC systems to be configured to dial home, which alerts EMC Global Service’s PSE Lab (Product Support Engineering) for the appropriate authorized EMC personnel to connect back to the EMC system for further troubleshooting and resolution. Configuring the EMC products to allow inbound dialing also enables EMC to proactively dial in to the EMC products, working to avoid problems by gathering needed diagnostic data or to attend to identified issues.

This section outlines the remote support security measures and practices EMC uses to assure customers that appropriate security safeguards have been put in place for the service and remote support process.

## ***EMC Centera Viewer and EMC Centera Command Line Interface***

The EMC Centera Viewer (CV) and the EMC Centera Command Line Interface (CLI) are the EMC Centera management tools that allow system operators and EMC personnel to monitor, diagnose, and manage a cluster. CV and CLI run on Windows and Solaris and do not require a dedicated workstation, as long as a secure IP connection can be established with the EMC Centera using the access nodes. These tools can also be used by directly connecting a workstation/laptop to a node that does not perform the access role. In this case, a cross-over cable must be used to connect with the EMC Centera internal subnet. The IP address of the workstation must be set to 10.255.0.2 or 172.19.0.2, depending on the subnet configuration, and the netmask is 255.255.255.252.

A number of default management profiles are defined on a 3.1 cluster: one for the local system administrator and two for EMC Service engineers. Each of these profiles has different levels of management capabilities based on the role of the individual support tiers. Those in EMC’s support organization with the most skill and responsibility can access the higher levels of capability.

EMC has documented guidelines for password composition and strength. Customer-specific practices for this application may be negotiated with the local support team.

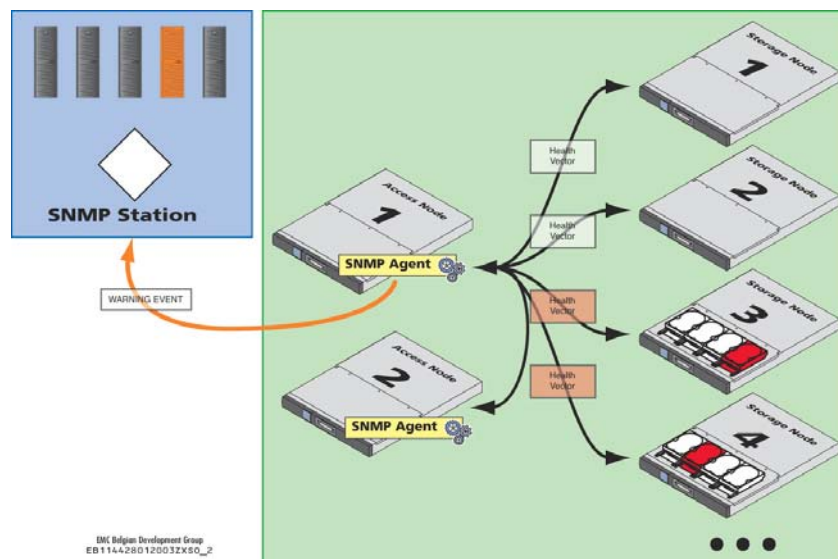
CV and CLI do not provide customers access to the data stored on EMC Centera and does not provide platform level access.

## Connect home using SMTP

This approach to providing remote support to EMC systems has been in place for years and has successfully served thousands of customers in all industries. The health check agent performs an ongoing check on the health of the cluster for errors or messages that the cluster needs to communicate to EMC for the appropriate response. The agent uses an SMTP connection to send health information and alerts back to EMC. The XML messages are encrypted using [FIPS 140](#) compliant encryption standards with AES (Advanced Encryption Standard) 256-bit strong encryption to meet the U.S. Department of Defense standards for security. The SMTP connection can be to a customer-provided SMTP gateway or to a dedicated ConnectEMC workstation.

## SNMP

The Simple Network Management Protocol ([SNMP](#)) is an Internet-standard protocol for managing devices on IP networks. It allows EMC Centera to communicate status, warning, and critical information to storage management software such as the EMC ControlCenter family. By default, SNMP is disabled for CE+ clusters, but it can be enabled by the system administrator.



The SNMP Agent runs only on access nodes:

- Traps are only sent by the principal access node.
- GET requests receive a no such OID message.
- GETNEXT commands get an End of MIB message.
- SET commands are not supported.

Figure 7. SNMP implementation

## MoPI

The Monitoring API (MoPI) is a part of the standard SDK and requires the access profile to be granted the monitor role. It is supported in all modes (Basic, GE, and CE+).

## Dial-in support

When EMC needs to remotely connect to the customer's site using EMC Centera Viewer or the CLI, it does so with a dial-in implementation that differs from the layered TCP/IP application mode. In the dial-in mode, there is specific client-side software handshaking that occurs between the dialer software that

---

authorizes EMC personnel to make the connection to EMC Centera. Successful handshaking between the EMC Support personnel's system and EMC Centera is required for any session to be enabled. The negotiation of that handshaking is encrypted (40-bit, proprietary method that is session specific) and must be successful in order to establish the PPP session. A potential attacker using [war dialing](#) techniques would not be rewarded with a session on the EMC Centera platform simply by discovering and dialing the phone number. After an EMC session is established, the normal EMC Centera cluster password negotiation will be used for authorization to service the customer's account.

Before any individual can initiate a call to a customer site, that person must pass several criteria. The person attempting the call is individually authenticated (multiple criteria are examined) and determined to be an appropriate member of the EMC Support team. Field-based personnel who might be known to the customer must still be properly associated with the specific customer's account in the EMC infrastructure. We recommend that modems are not connected continuously but are attached for the duration of the service intervention, unless the OnAlert™ workstation is used for remote connectivity.

### ***Controlled and audited platform access with sudo***

No root access to the Centera platform is possible. All platform access of EMC Service personnel is done through Super User Do ([sudo](#)), an open-source security tool that allows an administrator to restrict a user's ability to run certain commands. It also logs commands and arguments typed by specified system users. This log info is available to the system administrator through the Audit Logging functionality. The basic philosophy is to give as few privileges as possible but still allow people to properly support clusters in the field.

### ***OnAlert***

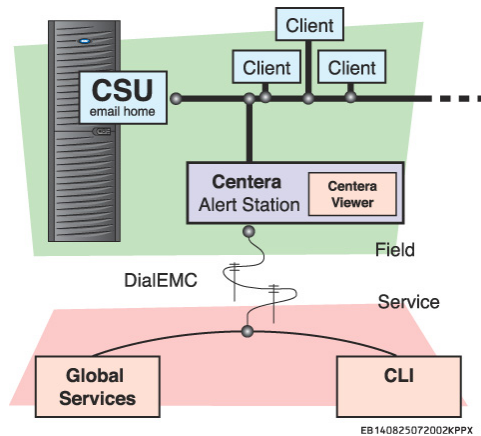
A dedicated OnAlert workstation can be installed to provide access to and from EMC for one or more Centera and other EMC storage devices, in addition to SMTP for connecting home and direct-attached modems for dial-in support. OnAlert Remote Service software is installed on an NT server/workstation to enable remote service capabilities to and from EMC Centera. Customers may segregate the server where OnAlert runs and use internally placed firewalls or other techniques to regulate inbound and outbound access to the rest of their Trusted Network. This approach could allow dial-out and dial-in connectivity for support, while ensuring only appropriate access to clusters for support purposes.

### **Connect home using OnAlert**

EMC Centera sends health and alert messages through SMTP to a local mail recipient on the OnAlert Station. The SMTP service then invokes DialEMC to forward the ConnectHome message file to Global Services using dialup, FTP, or SMTP transport (configurable).

### **Dial-In using OnAlert**

EMC Centera Viewer is also installed on an EMC Centera OnAlert station, which allows EMC Support engineers to remotely service a cluster from the OnAlert station using a dial-up connection.



**Figure 8. OnAlert setup**

## ***EMC Secure Remote Support Gateway***

The EMC Secure Remote Support Gateway is a secure, IP-based remote support infrastructure that can be implemented to remotely support EMC Centra clusters. It enables customers to actively participate in management of remote support—including authorization, authentication, and notification of “dial-in” and “connect home” access.

The EMC Secure Remote Support solution is an Internet-based infrastructure that will allow EMC Customer Service to provide dial-in and connect home product support at levels comparable to those of current modem-based connections.

The Gateway solution consists of two main components—gateway software that is installed at a customer site and enterprise management software that resides in an EMC data center. The gateway software, installed on a customer-supplied, dedicated server at a customer site, becomes the single point of entry and exit for all IP-based EMC remote support activity. Policy management software running on the gateway server or another customer-supplied server will allow customers to enforce authorization policies and audit connections to and from their network.

The enterprise management systems accept requests from a gateway and route connect home requests to the front-end processor or other EMC systems as appropriate. The enterprise server also serves as a bridge allowing EMC Support centers to establish secure, direct IP connections and remote control sessions with the gateway and the EMC products where it is installed.

The Gateway solution streamlines support with significant improvements. This IP-based, firewall-friendly messaging system initiates all connections from the customer site. Features include:

- **Increased Encryption for Transferred Data:** The Gateway will provide an increase in data transfer security to a minimum of 128-bit encryption to address the data privacy and integrity issues that customers currently face.
- **Centralized Authentication for Remote Access:** The EMC Secure Remote Support procedures and infrastructure will require anyone accessing a customer site to first be authenticated against EMC’s internal network. The Gateway will also require that customer access be limited to assigned EMC Support users and groups. Finally, customers will have device-level control of access to each installed EMC product.
- **Audit Logging:** Audit logging provides for a detailed record of remote access sessions, which will be maintained by both EMC and the customer.

---

## **Offsite EMC personnel connecting to EMC to provide customer support**

The customer's need for support at all times requires that EMC Support personnel access a cluster after properly authenticating themselves as members of EMC's support network, even if at a remote location. The support personnel, if remote, would begin by establishing a separate encrypted session for remote access to EMC. The EMC employee would first authenticate using [two-factor authentication \(SecurID from RSA Security\)](#) to gain access, and then authenticate again for their support role. The VPN tunnel uses a [Triple DES algorithm](#) (168 bit) and the IPSec protocol for connection to EMC. Critical to the added security is a mandated distributed firewall that is running continuously on the remote PC and is necessary to make a VPN connection to EMC. The distributed firewall rules are centrally managed by EMC at all times, as is PC virus protection. It is over a secured connection that the appropriate personnel may then initiate the call to a customer site. If the EMC Service personnel were at a different location from the customer, an outbound VPN connection to EMC would be made to allow the dial-in connection directly to the cluster for support. An alternative to off-campus EMC employee VPN tunnels is remote dial-in PPP connections to EMC, again using SecurID.

EMC is very sensitive to the importance of protecting proprietary and confidential information. As a result, all EMC employees are required to sign a key employee agreement that includes a nondisclosure agreement and agreement to customer confidentiality. The obligations of this agreement are binding and remain in effect even after termination of employment with EMC.

## **Data protection**

Customers may elect to handle the physical destruction of damaged or replaced drives according to their own internal practices; however, charges may apply due to the inability of EMC to make warranty claims.

## **Conclusion**

This white paper has covered the security architecture, measures, and practices of the EMC CentraStar server and EMC Centra SDK. New security-related features in the 3.x and 4.0 releases were introduced. The white paper covers the basic security principles: authentication using profiles and secrets, authorization provided by roles and capabilities, and auditing using the system logs. Service security is also covered.

## **References**

- Powerlink<sup>®</sup> access to EMC Centra Online Help can be found at:  
Home > Support > Technical Documentation and Advisories > Hardware/Platforms Documentation > Centra > CentraStar Operating System > General Reference > Centra Online help
- *EMC Centra Quick Start Guide*
- *EMC Centra SDK API Reference Guide*
- *EMC Centra SDK Programmer's Guide*