VMware AirWatch Content Rendering Engine Guide

For Linux

AirWatch v9.3

Have documentation feedback? Submit a Documentation Feedback support ticket using the Support Wizard on support.air-watch.com.

Table of Contents

Chapter 1:
Overview

Overview for AirWatch Content Management Enterprise Integration Solution

The AirWatch Content Management solution provides a suite of enterprise integration components designed to address the unique challenge of securing the content on mobile devices. The available AirWatch Content Management components include Content Gateway, Remote File Storage (RFS), and Content Rendering Engine (CRE).

AirWatch Content Gateway

The AirWatch Content Gateway, together with VMware Content Locker, lets your end users securely access content from an internal repository. This means that your users can remotely access their documentation, financial documents, board books, and more directly from content repositories or internal fileshares. As files are added or updated within your existing content repository, the changes will immediately be reflected in VMware Content Locker, and users will only be granted access to their approved files and folders based on the existing access control lists defined in your internal repository. Using the AirWatch Content Gateway with VMware Content Locker allows you to provide unmatched levels of access to your corporate content without sacrificing security. Install the latest Content Gateway version to ensure compatibility with the latest AirWatch Console versions.

Remote File Storage

Remote File Storage provides an on-premises storage alternative for Personal Content. Personal Content refers to a repository consisting of files uploaded and managed by end users. End users add files on their devices with AirWatch Content Locker, from any supported web browser with the Self-Service Portal, and from their personal computer with AirWatch Content Locker Sync. By default, this content is stored in the AirWatch Database. For SaaS customers, that means Personal Content stores in the cloud by default. In some use cases, storing certain types of content in the cloud poses a security risk. Use Remote File Storage (RFS) to store Personal Content in a dedicated on-premises location.Install the latest RFS version to ensure compatibility with the latest AirWatch Console versions.

Content Rendering Engine

The Content Rendering Engine (CRE) integrates with Remote File Storage to secure shared Personal Content. When an end user shares Personal Content from the Self-Service Portal, CRE converts the shared content into a rendered image of the source file. These shared images eliminate the need to download shared content, and enforce read-only permissions.

CRE enforces read-only permissions for the file types listed below:

- Word (doc, docx)
- Power Point (ppt, pptx)
- Excel (xls, xlsx)
- JPEG,JPG
- BMP
- PNG
- PDF
- Text

Available AirWatch Content Management Enterprise Integration Solutions

Before AirWatch v8.3, the Mobile Access Gateway (MAG) for Windows or VMware Tunnel for Linux products bundled enterprise proxy, per-app tunnel, and content services together. In AirWatch v8.3 and above, administrators looking to leverage the latest updates to content integration must migrate to the standalone content service known as Content Gateway.

The table below overviews the different versions of Content Gateway and Remote File Storage (RFS) available for install, the corresponding AirWatch Console version, and the availability of combined services.

Component	AirWatch Console Version					
	7.3	8.0	8.1	8.2	8.3	8.4+
Content Gateway						
VMware Tunnel	✓	✓	✓	✓		
Content Gateway					✓	✓
Standalone RFS						
v1.0*	✓					
v2.0		✓				
v2.1			✓			
v2.2				✓		
v2.3					✓	
v2.4+						✓
RFS with CRE**						
		✓	✓	✓	✓	✓
RFS behind Content Gateway						
						✓
RFS with CRE behind Content Gateway**						
						✓

*No fresh installations - continued support only

**Linux only

Overview for Content Rendering Engine Procedural

Use the overview to gain insight about the overall structure of the Content Rendering Engine (CRE) installation procedure, and the purpose of the different pieces involved in the procedure.

Install Remote File Storage (RFS)

Set up RFS storage so that CRE can render its files in the SSP. For instructions, see the **Remote File Storage Installation Guide** available in Accessing Other Documents on page 23.

Configure CRE

Configure CRE at a Customer level organization group in the AirWatch Console and download the installer.

Upload SSL Certificate

Use the manual utility to upload the SSL certificate saved as a PEM file to the RFS-Tokens server selected during configuration.

Install & Activate

Run the CRE installer on your server. Then, navigate to the AirWatch Console and manually activate CRE.

✓ **Verify**	Perform API healthchecks and other basic procedures to verify that installation occurred successfully.

Chapter 2:
CRE Architecture and Security

Overview of Architecture and Security

The Content Rendering Engine (CRE) is a product you can install on physical or virtual servers that reside in either the DMZ or a secured internal network zone. The Content Rendering Engine requires integration with the Remote File Storage solution.

Content Rendering Engine offers two architecture models for deployment: stand alone deployment with Remote File Storage or behind a AirWatch Content Gateway deployment for additional security. Both configurations support load-balancing for high availability and SSL offloading.

Configure your Content Rendering Engine deployment in a way that best addresses your security needs and existing setup. The variety of available options provides administrative flexibility when deciding on solution architecture.

Consider using a load balancer in the DMZ to forward traffic on the configured ports to an AirWatch component. Also consider using dedicated servers to eliminate the risk of other web apps or services causing performance issues.

Chapter 3:
CRE Installation Preparation

Requirements for Content Rendering Engine

Meet the minimum requirements to ensure a successful installation of Content Rendering Engine (CRE).

<table>
<tr><th>Requirement</th><th>Notes</th></tr>
<tr><td><b>VM or Physical Server (64-bit)</b></td><td>Co-locate CRE on a separate server in the same data-center or network as Remote File Storage (RFS) for maximum performance.</td></tr>
<tr><td><b>Sizing Recommendations</b></td><td>Sizing estimates for devices may vary based on concurrent usage. If CPU, RAM, or I/O utilization approaches 70-80%, consider adding more resources or servers.
<table>
<tr><th># of Devices</th><th>CPU Cores</th><th>RAM (GB)</th><th>Disk Space (GB)</th></tr>
<tr><td><b>1-1000</b></td><td>4+</td><td>4-8</td><td>20+</td></tr>
<tr><td><b>1,000-5,000</b></td><td>8-16 CPU cores
OR
4 CPU cores w/4 load-balanced servers</td><td>8-16</td><td></td></tr>
<tr><td><b>5,000-25,000</b></td><td>16 CPU cores w/4 load-balanced servers OR
8 CPU cores w/8 load-balanced servers</td><td>16-32</td><td></td></tr>
<tr><td><b>25,000+</b></td><td>8-16 CPU cores w/8-16+ load-balanced servers</td><td>32+</td><td></td></tr>
</table>
</td></tr>
</table>

General Requirements

Requirements	Notes
Internally registered DNS record	Register the Endpoint server.
Externally registered DNS record	Register the Endpoint server.
SSL Certificate from trusted third party with subject name of server hostname	Requires a PKCS12 (.pfx) format and the trust of all device types in use. Keep in mind: • Android does not natively trust all Comodo certificates. • PKCS12 (.pfx) format includes the server certificate, private key, root chain, and password protection.
Remote File Storage set up and configured	Because CRE integrates with RFS for Linux, you must install RFS for Linux before proceeding with CRE installation. For more information, see the **VMware AirWatch Remote File Server Guide for Linux**.

Software Requirements

Requirement	Notes
SSH access to Linux Servers and an admin account with full write permissions.	Root permissions, or sudo access with the same privileges as root required. Once installation completes, you can put restrictions into place for these account types.

Requirement	Notes
yum Enabled	Enable to allow the installer to request and install any missing prerequisites.
CentOS 7.1/7.2/7.3/7.4 **RHEL 7.1/7.2/7.3/7.4 (Non-licensed servers are not supported for Content Gateway installation)** **SLES 12 (SP1/SP2/SP3)**	UI-less recommended. Basic infrastructure type recommended.

Network Requirements

Source Component	Destination Component	Protocol	Port	Configurable	Notes
AirWatch Console	AirWatch CRE	HTTPS	443	Yes	Post-installation, activate CRE in the AirWatch Console to verify success.
DS Server	AirWatch CRE	HTTPS	443	Yes	Post-installation, activate CRE in the AirWatch Console to verify success.
Devices (from Internet and Wi-Fi)	AirWatch CRE	HTTPS	443	Yes	Post-installation, use a diagnostic endpoint to verify availability.
CRE Server	RFS Load Balancer or HA Proxy	HTTPS	443	Yes	
CRE Server	Other CRE Servers in cluster	TCP	5701	Yes	Hazelcast opens the port 5701 by default, and follows this +1 naming convention for all subsequent ports. Post-installation, use diagnostic endpoints to verify availability.

Chapter 4:
CRE Configuration

Configure the Content Rendering Engine

Configure Content Rendering Engine (RFS) settings in the AirWatch Console to establish a connection from CRE to Remote File Storage (RFS) and pre-configure the settings files that get bundled into the installer, eliminating the need to manually configure them post-installation on the server.

1. Navigate to **Content > Settings > Content Viewer**, at a Customer level Organization Group.
2. Select **Configure** if configuring the first CRE instance. After the first instance, the option switches to **Add**.
3. On the **Assignment** screen, select an **RFS Node** from the same data-center or network as CRE to have content rendered in the SSP. AirWatch recommends limiting one CRE instance per RFS node. Select **Next**.
4. Configure the fields on the **Details** screen. Select **Next**.

Setting	Description
Name	Provide a name for the content viewer. This name displays in the AirWatch Console.
CRE URL	Provide the externally accessible URL for the CRE you set up on your server.

5. Assign a **Public SSL Certificate** on the **Authentication** screen to establish trust between RFS and the Content Viewer. Select **Next**.
6. Select the **Edit** icon ✎ from the actions menu for the CRE node.
7. Select the **Advanced** tab.
   - Copy and record the **Client ID**.
   - Select **Generate PEM**. Copy and paste the text into a text editor, saving it as a .pem file.

     Example: Save the text as **CreClientCertificate.pem**.
8. Review the **Summary** screen. Select **Save** after reviewing the newly configured settings.
9. Select **Download** under the **Installer** column and follow the prompts.
10. Use the manual utility to upload the SSL certificate to the RFS Tokens server selected during configuration.

Remote File Storage Manual Utility

Use the Remote File Storage (RFS) manual utility, pre-packaged within the RFS-Web module, to manually upload certificates. Client and regenerated certificates for Content Rendering Engine (CRE) as well as regenerated RFS certificates require the use of the manual utility.

Review the commands and the explanation of the command's components to gain insight about the information needed to manually add an RFS or CRE certificate to the the RFS-Web server.

Command Line and Components		
OS	**Command**	
Linux	`sh /opt/airwatch/rfs/rfs-web/etc/unix/rfs-cert-util.sh –cn ALIAS_NAME –cp CLIENT_CERTIFICATE_FILE –fp TRUSTSTORE_PATH –t yes`	
Component	**Description**	**Notes**
ALIAS_NAME	The **Client ID** for the certificate.	Do not use spaces.
CLIENT_ CERTIFICATE_ FILE	The uploaded .pem file's location.	
TRUSTSTORE_ PATH	The path to the directory that contains the truststore folder, located by default under the RFS file storage path at subdirectory: **/truststore/**.	Verify the file storage or truststore path by reviewing the **aw.filesystem.root** and **aw.truststore.path** values found at **/opt/airwatch/rfs/rfs-web/config/rfs.properties** on Linux .

Upload a Content Rendering Engine Certificate

Use the Remote File Storage (RFS) manual utility, pre-packaged within the RFS-Web module, to manually upload certificates to a shared truststore instance. The manual utility handles client certificates for Content Rendering Engine (CRE) as well as regenerated RFS and CRE certificate uploads.

Process Overview

1. Transfer the .pem file to the truststore path on the appropriate RFS-Web server.
2. Run the appropriate command from a server with the RFS-Web component installed.
3. If the notification **Certificate was added to keystore** appears, restart all services to complete the process.

   If the notification **<name> truststore … does not exist. Creating <name> truststore path** appears, delete the newly created truststore folder, adjust the –fp path, and rerun the command.

CRE Components

Use the specified component values and associated instructions to gain insight into how the manual certificate upload process works. Do not view the provided values as recommendations. The example defines the components as absolute paths for the sake of clarity.

Component	CRE
Manual Certificate Utility Name	rfs-cert-util.sh
Manual Certificate Utility File Location	/opt/airwatch/rfs/rfs-web/etc/unix/
ALIAS_NAME	Acme_Production_Cre_Cert
CLIENT_CERTIFICATE_FILE	/mnt/RFS_Storage/CreClientCertificate.pem

Component	CRE
TRUSTSTORE_PATH	/mnt/RFS_Storage/
.pem File Name	CreClientCertificate.pem

Upload Process

Review how to upload a CRE certificate on a Linux RFS-Web server.

1. Transfer the **RfsClientCertificate.pem** file to the **/mnt/RFS_Storage/truststore/** on the RFS-Web servers.
2. Run the command from a Linux server with the RFS-Web component installed.

```
sh /opt/airwatch/rfs/rfs-web/etc/unix/rfs-cert-util.sh -cn 98cfa7ef-4e2f-14d2-
8134-efa03e34748c -cp /mnt/RFS_Storage/truststore/CreClientCert.pem -fp
/mnt/RFS_Storage/
```

3. Review the **Certificate was added to keystore** notification that appears, indicating the certificate uploaded successfully. Restart the RFS Service to complete the process.

View Successfully Uploaded Certificates

Generate a .txt file to review certificates sucessfully uploaded to the keystore.

1. Change your command line working directory to the truststore directory and execute the following command:

```
keytool -list -v -keystore rfs.jks > keystoreContents.txt
```

2. When prompted to enter a password, press **Enter**.
3. Open and review the resulting .txt file.

Chapter 5:
CRE Installation

Install Content Rendering Engine on Linux

Install Content Rendering Engine (CRE) so that end users can securely share content as an image from the Self-Service Portal. After configuring CRE in the AirWatch Console, download the installer and proceed with installation.Complete the following steps to install CRE on the Linux Server. AirWatch recommends installing Redis and CRE on separate servers utilizing the GUI-less method outlined in these instructions.

1. Copy the file you downloaded from the AirWatch Console into a folder in the Linux server.
2. Navigate to the folder you copied the file to in the Linux box. Un-archive the .tar file using the following command:

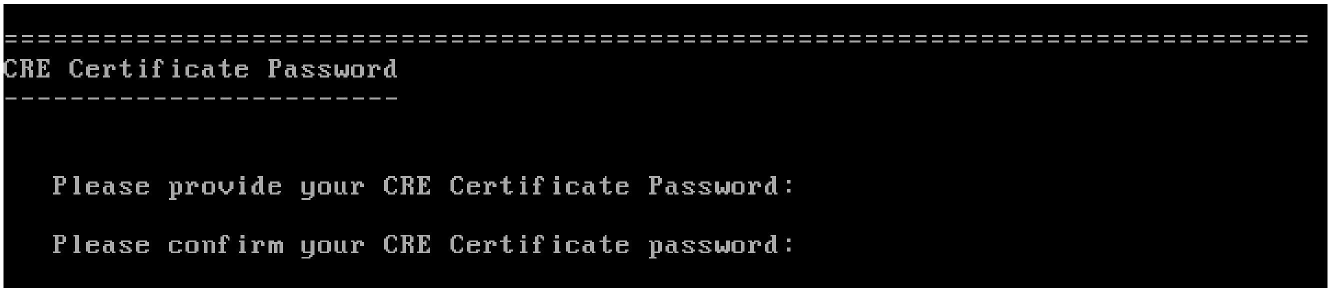
```
unzip CREInstaller.zip
```

3. Open the un-zipped installation folders:
   - config.xml
   - ContentRenderingEngine.bin
   - rest-ssl-cert.pfx
   - rfs-plugin-cert.pfx
4. Make the **ContentRenderingEngine.bin** an executable using the following command:

```
sudo chmod +x ContentRenderingEngine.bin
```

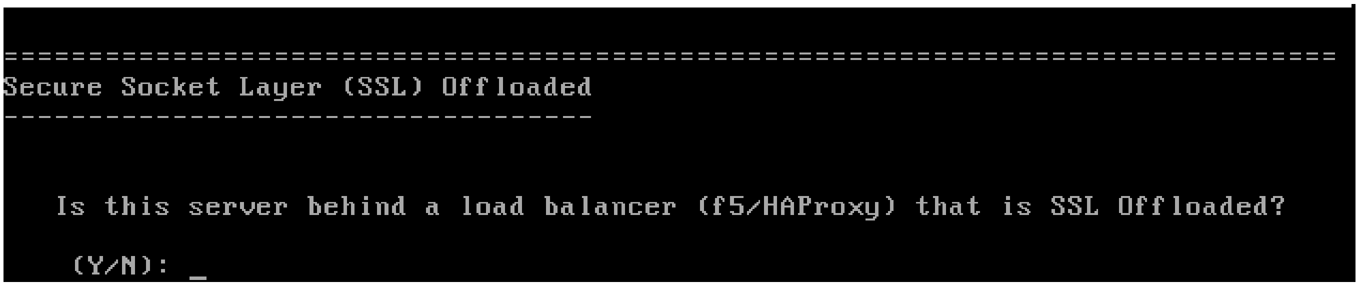
```
sudo ./ContentRenderingEngine.bin
```

5. Review the Introduction that appears during an initial installation.
6. Select **Continue** and accept the licensing agreement. Press **Y** to accept.
7. Enter and confirm the **Certificate Password** you entered when downloading the configuration file from the AirWatch Console.



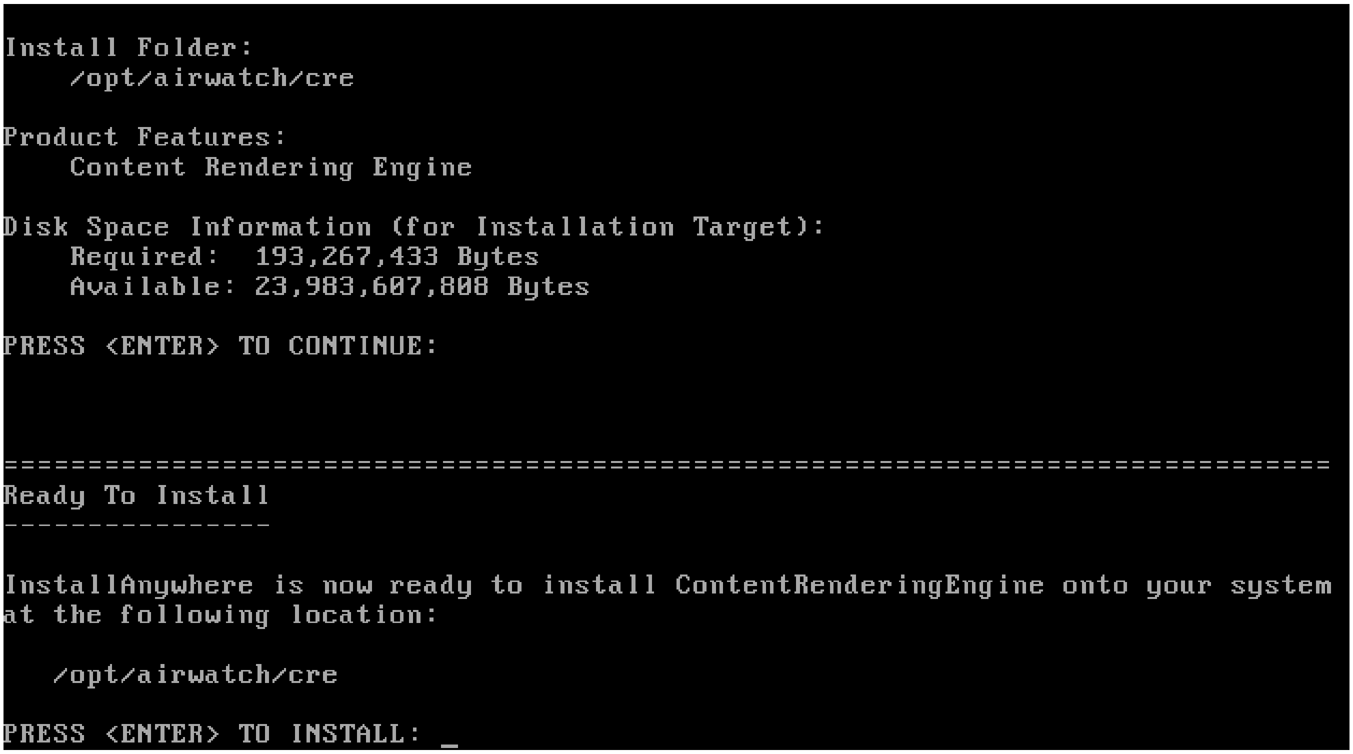
```
===============================================================================
CRE Certificate Password
------------------------


   Please provide your CRE Certificate Password:

   Please confirm your CRE Certificate password:
```

8. Enter **Y** to confirm the server is **Secure Socket Layer (SSL) Offloaded**. Enter **N** if your server is not behind an SSL offloaded load balancer.



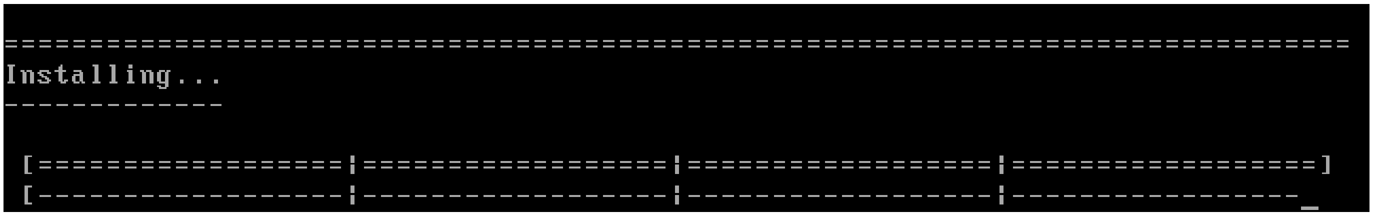
```
===============================================================================
Secure Socket Layer (SSL) Offloaded
-----------------------------------


   Is this server behind a load balancer (f5/HAProxy) that is SSL Offloaded?

    (Y/N): _
```

9. Review the **Summary** information for accuracy. Press **Enter** to continue.



```
Install Folder:
    /opt/airwatch/cre

Product Features:
    Content Rendering Engine

Disk Space Information (for Installation Target):
    Required:  193,267,433 Bytes
    Available: 23,983,607,808 Bytes

PRESS <ENTER> TO CONTINUE:



===============================================================================
Ready To Install
----------------

InstallAnywhere is now ready to install ContentRenderingEngine onto your system
at the following location:

   /opt/airwatch/cre

PRESS <ENTER> TO INSTALL: _
```

10. Press **Enter** to begin installation. Any install errors display in an error message, and in the installation log which saves in the same directory as CRE. Press **Enter** to exit the installer.



```
===============================================================================
Installing...
-------------

 [==================|==================|==================|==================]
 [------------------|------------------|------------------|-----------------_
```

11. Once the installation is complete, you can check that the CRE service is running by using the following command:

```
$ sudo service cre status
```

12. In the AirWatch Console, navigate to **Content > Settings > Content Viewer.**Select **Activate**. If successful, the icon turns green. Otherwise, the install failed and you need to troubleshoot before proceeding.

Verify Content Rendering Engine Connectivity

Post-installation, perform checks to verify the installation completed successfully.

1. Verify CRE connectivity to RFS by entering the following command:

```
curl -I <rfsURL>/awhealth
```

2. Use a browser on a different machine within the same network to check the health API endpoint availability.

	HTTP GET request to	Return HTTP status	Service Status
CRE	<CRE_URL>:<PORT>/awhealth	200 status with the CRE version	UP

Upgrade Content Rendering Engine

Follow the upgrade procedure to access the most current version of the Content Rendering Engine (CRE).

1. Log in to the AirWatch Console and navigate to **Content > Settings > Content Viewer**.
2. Find the CRE node you want to upgrade and then select the **Download** hyperlink under the Installer heading.
3. Enter and confirm a **certificate password** and then click **Download**.
4. Perform the for the CRE server component.

Chapter 6:
CRE Management

Add Content Rendering Engine Nodes

The procedure for adding additional Content Rendering Engine (CRE) servers mimics the initial configuration process, but includes two additional requirements.

Add an additional server by completing the following steps:

1. Navigate to **Content > Settings > Content Viewer** in a *Customer Level* Organization Group.
2. Select **Add**.
3. Follow the steps for .
    - Limit one CRE configuration per Remote File Storage (RFS) configuration
    - Co-locate CRE and RFS in the same data-center or network

Regenerate Content Rendering Engine Certificates

Regenerate certificates in the AirWatch Console. Save the certificate as a .pem file to convert it into the format required when uploading to the RFS-Web server.

1. Select the **Edit** icon ✎ from the actions menu for the CRE node.
2. Select the **Advanced** tab.
3. Under the AirWatch Client Certificate section, select the **Regenerate** button.
4. Copy and record the **Client ID**.
5. Select **Generate PEM**. Copy and paste the text into a text editor, saving it as a .pem file.

   Example: Save the text as **CreClientCertificate.pem**.

Uninstall Content Rendering Engine on Linux

Run the following commands to uninstall a previously installed CRE server:

1. Navigate to the **/opt/airwatch/cre/_ContentRenderingEngine_installation/** directory.

```
cd /opt/airwatch/cre/_ContentRenderingEngine_installation
```

2. Execute the uninstall script.

```
sudo ./UninstallContentRenderingEngine
```

Troubleshooting Resources for Content Rendering Engine

Use the available installation logs, server logs and configuration files to troubleshoot Content Rendering Engine (CRE). Access these resources from their directory location or by entering server commands on the vi editor.

Name	Location
Directories	
Post-Installation Log	/opt/airwatch/cre/_ContentRenderingEngine/Logs/
Server Logs	/var/log/airwatch/cre
Configuration Files Default Directory	/opt/airwatch/cre/conf
CRE Properties File	/opt/airwatch/cre/conf/cre.properties
CRE logback.xml File	/opt/airwatch/cre/conf/logback.xml
Commands	

Read a Log File	`$ cd /var/log/airwatch/cre`
	`$ tail -f cre.log`

Read a Log File	`$ cd /var/log/airwatch/cre`
	`$ tail -f cre.log`

Set Logging Levels

Follow the steps below to change logging levels.

1. Access the **logback.xml** file contained in the RFS Configuration Folder.
2. Edit the file on using the Linux vi editor or on WinSCP:
3. Write text in the logback.xml file:
   - Enter **i** to begin writing text.
   - Change the **logging level** XML attribute value in both logger and root XML elements.
   - Press **Esc** to exit edit.
   - Press **:wq!** to write and quit.
4. **Restart** each service after saving changes.

Accessing Other Documents

While reading this documentation you may encounter references to documents that are not included here.

The quickest and easiest way to find a particular document is to navigate to https://my.air-watch.com/help/9.2/en/Content/Release_Notes/Doc_List_PDFs.htm and search for the document you need. Each release-specific document has a link to its PDF copy on AirWatch Resources.

Alternatively, you can navigate to AirWatch Resources on myAirWatch (resources.air-watch.com) and search. When searching for documentation on Resources, be sure to select your AirWatch version. You can use the filters to sort by PDF file type and AirWatch v9.3.