Remote File Storage for Linux

VMware Workspace ONE UEM 1903

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

Content Management Enterprise Integration Solution

1

The 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 Content Management components include Content Gateway, Remote File Storage (RFS), and Content Rendering Engine (CRE).

Content Gateway

The Content Gateway, together with VMware Workspace ONE Content, 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 file shares. As files are added or updated within your existing content repository, the changes will immediately be reflected in VMware Workspace ONE Content, 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 Content Gateway with VMware Workspace ONE Content allows you to provide unmatched levels of access to your corporate content without sacrificing security.

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 VMware Workspace ONE Content, from any supported web browser with the Self-Service Portal, and from their personal computer with Content Locker Sync. By default, this content is stored in the Workspace ONE UEM 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.

Note   VMware Workspace ONE has announced January 3rd, 2020 as the End of Life (EOL) date for Personal Content and its related features. For more information about the end of life announcement, see End of General Support for VMware Workspace ONE Personal Content.

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 following file types.

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

This chapter includes the following topics:

- Available Content Management Enterprise Integration Solutions
- Remote File Storage for Personal Content
- Remote File Storage Procedural Overview

Available Content Management Enterprise Integration Solutions

Before console 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 console 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 UEM console version, and the availability of combined services.

|	UEM Console Version					
Component	**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					✓	

Component	UEM Console Version					
	7.3	8.0	8.1	8.2	8.3	8.4+
v2.4+						✓
RFS with CRE**						
		✓	✓	✓	✓	✓
RFS behind Content Gateway						
						✓
RFS with CRE behind Content Gateway**						
						✓

*No fresh installations - continued support only

**Linux only

Remote File Storage for Personal Content

Personal Content stores in the Workspace ONE UEM database by default. However, SaaS and on-premises customers with concerns about security of personal data can install Remote File Storage to create a dedicated, on-premises storage solution for Personal Content.

Use the diagram to gain insight into how Remote File Storage works for Personal Content.
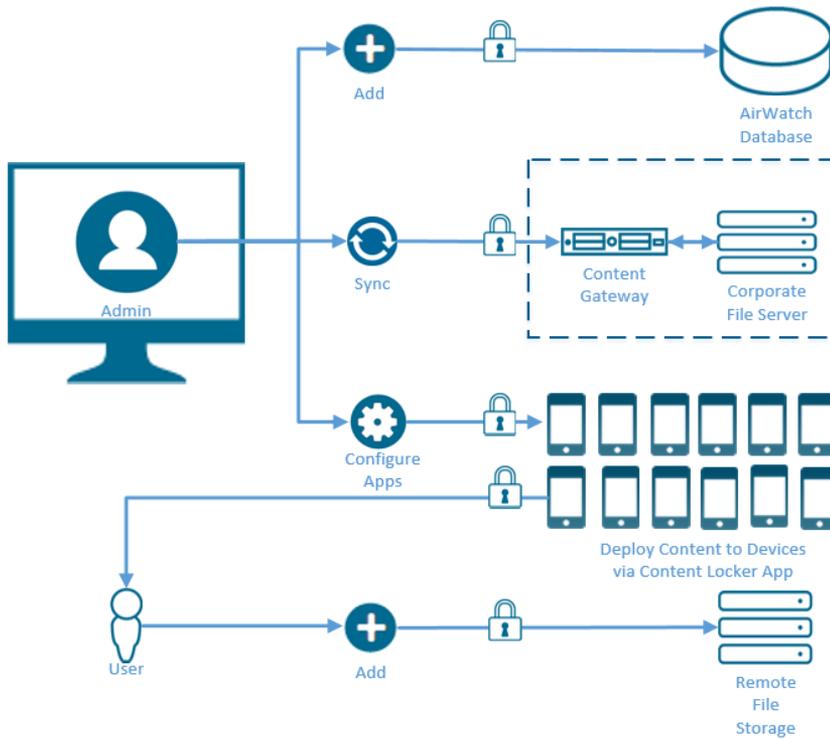
Important VMware Workspace ONE has announced January 3rd, 2020 as the End of Life (EOL) date for Personal Content and its related features. For more information about the end of life announcement, see End of General Support for VMware Workspace ONE Personal Content.

Remote File Storage Procedural Overview

Use the overview to gain insight about the overall structure of the Remote File Storage (RFS) installation procedure, as well as the purpose of the different pieces involved in the procedure.

	Configure	Configure an RFS instance in the UEM Console and download the installer.
	Install	Open the installation package on your server, and follow the prompts to install RFS.
	Verify	Perform API healthchecks and other basic procedures to verify installation occurred successfully.

Architecture and Security

2

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 VMware 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 a Workspace ONE UEM component. Also consider using dedicated servers to eliminate the risk of other web apps or services causing performance issues.

Remote File Storage Architecture

RFS connects directly with the internal resources over non-standard ports, which might raise concerns for administrators who do not want those ports exposed.

Directing device traffic to Content Gateway makes RFS an internal only resource by passing off the external exposure to Content Gateway.

Review the basic setup, benefits, and considerations for scalable architecture.
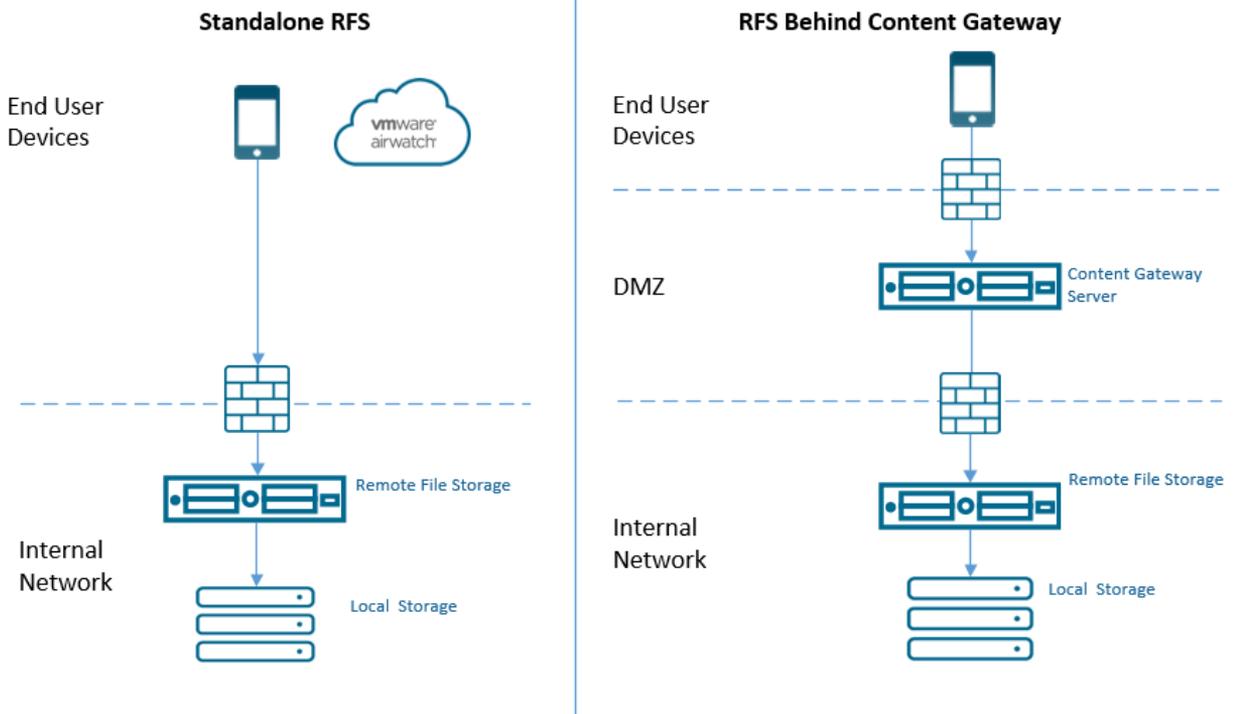
RFS Installation Preparation

<div align="right">

3

</div>

Meet the minimum hardware, general, software, and network requirements to ensure a successful installation. You can also verify the RFS path before starting the installation.

Hardware Requirements

Requirement	CPU Cores	RAM (GB)	Disk Space	Notes
VM or Physical Server (64-bit)	2 CPU Core (2.0+GHz)	4 GB+	20+ GB	Sizing is an estimate and may vary based on your concurrent usage. Consider adding more resources or servers when CPU, RAM, or I/O utilization approaches 70-80%.

Number of Devices	1-1,000	1,000-5,000	5,000-25,000	25,000+
CPU Cores	2	4-8 or 2 load-balanced servers w/ 2 CPU cores	2 load-balanced servers w/8 CPU cores or 4 load-balanced w/ 4 CPU cores	4-8+ load-balanced servers with 4-8 CPU cores
RAM (GB)	4	8-16 total	16-32 total	32+ total

General Requirements

Requirements	Notes
Internally registered DNS record	Register the Endpoint server. Required for Standalone RFS **and** RFS with Content Gateway.
Externally registered DNS record	Required for Standalone RFS only.
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.
Dedicated storage location that supports NFS or CIFS	Serves as the location where RFS stores files.
Enable Multi-casting	Recommended, not required. Multi-casting is a network protocol that allows RFS servers to detect and communicate with one another.

Software Requirements

For configuring the ports listed below, all the traffic is uni-directional (outbound) from the source component to the destination component.

Table 3-2. Standalone RFS Network Requirements

Source Component	Destination Component	Protocol	Port	Configurable	Notes
UEM Console & DS Server	RFS Server	HTTPS	443	Yes	Post-installation, activate RFS in the UEM console to Verify Remote File Storage Connectivity connectivity.
Devices (from Internet and Wi-Fi)	RFS Server	HTTPS	443	Yes	Post-installation, use health API's to Verify Remote File Storage Connectivity endpoint availability.
RFS Server	Other RFS Servers in cluster	TCP	5701, 5702	Yes	Installing files and tokens on the same server opens two Hazelcast ports. Hazelcast opens the port 5701 by default, and follows this +1 naming convention for all subsequent ports. Post-installation, use diagnostic endpoints to Verify Remote File Storage Connectivity availability.
RFS Server	NFS storage component -OR- CIFS storage component	TCP/UDP	2049, 111	No	Required if using a NFS share. Prior to installation, Verify the Remote File Storage Path ports.
		TCP	137-139, 445	No	Required if using a CIFS share. Prior to installation, Verify the Remote File Storage Path ports.

Table 3-3. RFS Behind Content Gateway Network Requirements

Source Component	Destination Component	Protocol	Port	Configurable	Notes
Content Gateway Endpoint	RFS Server	HTTPS/HTTP	443, 80	Yes	
RFS Server	Other RFS Servers in cluster	TCP	5701, 5702	Yes	Installing files and tokens on the same server opens two Hazelcast ports. Hazelcast opens the port 5701 by default, and follows this +1 naming convention for all subsequent ports. Post-installation, use diagnostic endpoints to Verify Remote File Storage Connectivity availability.

Table 3-3. RFS Behind Content Gateway Network Requirements (Continued)

Source Component	Destination Component	Protocol	Port	Configurable	Notes
RFS Server	NFS storage component -OR- CIFS storage component	TCP/UDP	2049, 111	No	Required if using a NFS share. Prior to installation, Verify the Remote File Storage Path ports.
		TCP	137-139, 445	No	Required if using a CIFS share. Prior to installation, Verify the Remote File Storage Path ports.

Verify the Remote File Storage Path

Verify that the path to the drive you mounted to a NAS share functions properly.

Procedure

1 Enter the command to ensure the file system mounted.

    df –h

2 Make sure the space you have available is greater than or equal to the storage quota you configured in the UEM console for RFS in the values that return.

Filesystem	Size	Used	Available	Use%	Mounted On
/dev/sda	28G	3.8G	23G	15	/
10.43.22.185:/airwatch/rfs	500G	22G	478G	5	/mnt/rfs

RFS Configuration

4

Download the Remote File Storage Server (RFS) executable in the UEM Console. Once downloaded, install RFS by running the executable. Then, return to the UEM Console and verify the installation completed successfully.

Procedure

1   Navigate to **Groups & Settings > All Settings > Content > Remote Storage**.

2   Select **Configure** if you are setting up the first instance of RFS.

3   Complete the fields in the **Details** screen that appears. Select **Next** to continue.

Settings	Descriptions
Name	Provide a unique name to identify the RFS server. When installing multiple RFS nodes, provide each with a name specific to the region of installation.
RFS URL	Supply the full URL to the externally accessible RFS. Specify http or https in URL and include the Port if not using 443 or 80.
Access via Content Gateway	Leave disabled to implement standalone RFS. Enable to utilize RFS behind Content Gateway.
ICAP Proxy Configuration	For information about configuring ICAP Proxy, see https://support.workspaceone.com/articles/115001675368. **Note** New ICAP Proxy configurations are not supported from Workspace ONE UEM console version 9.7. Existing configurations can be edited.

4   Complete the fields in the **Storage** screen that appears. Select **Next** to continue.

Settings	Descriptions
Storage Quota	Set the maximum amount of storage in GB that the RFS node accepts. Workspace ONE UEM ensures the storage quota does not exceed the storage location's limits.
Maximum File Size	Set the maximum individual file size allowed for upload to the RFS node. Workspace ONE UEM supports files up to 8 GB in size.

5   Upload the **Public SSL Certificate** associated with RFS URL from the authentication screen.

6   Enter the certificate's password and select **Upload** to continue.

7   Select the appropriate OS **Download** to download the installer.

8   Create a certificate password with a minimum of 6 characters. Confirm your entry.

9   Select **Download**, then **Save**.

RFS Installation

5

Before you begin with the RFS installation, understand the compatibility of Remote File Storage (RFS) with the current and previous versions of the UEM console and Content Gateway.

Remote File Storage Compatibility Matrix

RFS for Linux

Console Version	Content Gateway for Linux Version	RFS Version
1810	2.6	2.7
9.7	2.6	2.7

This chapter includes the following topics:

- Installing RFS on Linux
- Verify Remote File Storage Connectivity
- Upgrade from Remote File Storage v2.4 and Above

Installing RFS on Linux

Workspace ONE UEM supports installation of RFS on Linux and Windows servers. You can also verify the installation using the options provided in the UEM console.

Complete the following steps to install RFS on the Linux Server. Workspace ONE UEM recommends utilizing the GUI-less method outlined in these instructions.

Procedure

1   Copy the .zip file you downloaded from the UEM console into a folder in the Linux server.

2   Navigate to the folder you copied the file to in the Linux box. Unzip the file.

```
unzip RFSInstaller.zip
```

3   Open the un-zipped installation folders.

- config.xml

- RemoteFileStorage.bin

- rfsSSl.pfx

4 Make the **RemoteFileStorage.bin** executable.

```
sudo chmod +x RemoteFileStorage.bin
```

```
sudo ./RemoteFileStorage.bin
```

5 Press **Enter** until you receive a prompt to accept the licensing agreement. Press **Y** to accept.

6 Respond to the prompts in the **RFS Configuration** section.

a Enter **Y** to utilize automatic communication using multi-casting.

Alternatively, enter **N** to cluster RFS servers by host name, and provide the IP addresses for the servers.

b Enter **Y**. Enter **N**.

c Enter **Y** if the RFS server gets SSL offloaded behind a load balancer. Otherwise, enter **N**.

7 Enter and confirm the **Certificate Password** you entered when downloading the installer in the console.

8 Configure the **RFS Storage** file path.

a Enter the **absolute path** where RFS stores files, which should match the path created when RFS was configured.

b Review your entry.

c Press **Y** to confirm.

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

10 Press **Enter** to begin installation.

Any install errors display in an error message, and in the installation log which saves to

```
opt/airwatch/rfs/_RemoteFileStorage_installation/logs
```

.

11 Run the command to check that all the services run properly.

```
$ sudo service AirWatchRfs status
```

12 Verify RFS installed successfully.

For more information, see Verify Remote File Storage Connectivity.

Verify Remote File Storage Connectivity

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

Procedure

1 Verify the RFS installation completed successfully by checking the **\\<servername > \<path >** for the trust store folder.

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
RFS Tokens	<RFS_HOSTNAME>:<PORT>/awhealth	200 status with the RFS version	UP
Hazelcast	http://localhost:60010/diagnostics	200 status with cluster details	UP

3 Navigate to **Groups & Settings > All Settings > Content > Remote Storage** in the UEM console.

4 Check the **Active** column for the appropriate RFS node. The color that displays in the column indicates the node's connectivity status.

Color	Meaning
Blank	Indicates default node status. The blank status appears regardless of connectivity.
Green	Indicates active status.
Red	Indicates an inactive status. Troubleshooting Resources for Remote File Storage before proceeding.

Upgrade from Remote File Storage v2.4 and Above

Upgrade Remote File Storage(RFS) to access the most current version of the installer.

You can opt out of an upgrade to continue use of the existing implementation without disruption. To opt out, simply leave the installer configurations the same, and do not download the installer available in .

Procedure

1 Navigate to **Groups & Settings > All Settings > Content > Remote Storage**.

2 Select the **Download** hyperlink for the RFS node you want to upgrade.

3 Enter and confirm a certificate password and select **Download**.

4 Open the file you downloaded from the UEM console and run the installer.

- If upgrading **Remote File Storage for Linux**, follow the Linux Installing RFS on Linux.

- If upgrading **Remote File Storage for Windows**, follow the Windows installation procedure.

Add Remote File Storage Nodes

6

Workspace ONE UEM provides you different options to manage your RFS environment. You can manage your Remote File Storage Server (RFS) nodes, regenerate certificates for RFS, upload regenerated certificate or map user groups using the options provided in the UEM console.

Use multiple RFS instances to store Personal Content in multiple regions.

Procedure

1   Navigate to **Groups & Settings > All Settings > Content > Remote Storage** in a Customer Level Organization Group.

2   Select **Add** (RFS 2.0+).

3   Configure RFS.

  For more information, see Chapter 4 RFS Configuration

This chapter includes the following topics:

- Regenerate Remote File Storage Certificates

- Map User Groups to Remote File Storage Nodes

- Remote File Storage Manual Utility

- Upload a Regenerated Remote File Storage for Linux Certificate

- Troubleshooting Resources for Remote File Storage

- Set Logging Levels

Regenerate Remote File Storage Certificates

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

Procedure

1   Select the **Edit** icon from the actions menu for the RFS 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.

Save the text as **RfsClientCertificate.pem**.

Map User Groups to Remote File Storage Nodes

By default, your Remote File Storage (RFS) instance stores personal content for the organization group you configured it in. Assign user groups to distinguish assignment within an organization group. Unassigned user groups map to the primary RFS instance.

Procedure

1   Navigate to **Groups & Settings > All Settings > Content > Remote Storage**.

2   Select **Edit User Group Assignments**.

3   Select **Add Assignment**.

4   Assign a **User Group** and an **RFS Node** from the drop-down menus. Select the **Add** icon to add additional entries if you need to.

5   Select **Save**.

Remote File Storage Manual Utility

Use the Remote File Storage (RFS) manual utility, pre-packaged within the RFS-Web module, for manually uploading certificates. Client and regenerated certificates for Content Rendering Engine (CRE) and 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 for manually adding an RFS or CRE certificate to 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 Regenerated Remote File Storage for Linux 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.

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.

Table 6-1. Linux Components

Component	Linux
Manual Certificate Utility Name	rfs-cert-util.sh
Manual Certificate Utility File Location	/opt/airwatch/rfs/rfs-web/etc/unix/
ALIAS_NAME	98cfa7ef-4e2f-14d2-8134-efa03e34748c
CLIENT_CERTIFICATE_FILE	/mnt/RFS_Storage/RfsClientCertificate.pem
TRUSTSTORE_PATH	/mnt/RFS_Storage/truststore/
.pem File Name	RfsClientCertificate.pem

Procedure

1 Transfer the **RfsClientCertificate.pem** file to the **/mnt/RFS_Storage/truststore/** on the RFS-Web servers.

2 Run the appropriate 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/RfsClientCert.pem –fp /mnt/RFS_Storage/
```

The **Certificate was added to keystore** notification should appear, indicating the certificate uploaded successfully.

3 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.

4 Restart all RFS Services to complete the process.

Troubleshooting Resources for Remote File Storage

To troubleshoot Remote File Storage (RFS), use the available installation logs, server logs, and configuration files. Access these resources from their directory location or enter server commands on the vi editor or WinSCP.

Name	Details
Directories	
Post-Installation Log	/opt/airwatch/rfs/_RemoteFileStorage_installation/Logs/
Server Log	/var/log/airwatch/rfs
RFS Configuration Files Default Directory	rfs_web/config
RFS-Web Property File	/opt/airwatch/rfs/rfs-web/config/rfs.properties
RFS Files Property File	/opt/airwatch/rfs/rfs-files/config/rfs.properties
Commands	
Read a Log File	```[root@localhost ~]$ cd /log/airwatch/rfs/``` ```[root@localhost vpnd]$ tail -f rfs-web.log```
View a Directory Listing	```[root@localhost ~]$ cd /opt/airwatch/rfs``` ```[root@localhost vpnd]$ ls -l```
RFS Service Commands	```sudo service AirWatchRfs {start/stop/restart/status}```

Set Logging Levels

You can change the logging levels that are set in the logback.xml file contained in the RFS Configuration Folder.

Procedure

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 the text in the logback.xml file.

   a   Enter **i** to begin writing text.

   b   Change the **logging level** XML attribute value in both logger and root XML elements.

   c   Press **Esc** to exit edit.

   d   Press **:wq!** to write and quit.

4   **Restart** each service after saving changes.

Options	Description
Restart RFS	```sudo service AirWatchRfs restart```