QuickFile

# Administration Guide

*Version 1.1*

QuickFile

# Administration Guide

*Version 1.1*

**Note**
Before using this information and the product it supports, read the information in "Notices" on page 101.

This edition applies to version 1.1 of QuickFile (product number 5725-F81) and to all subsequent releases and modifications until otherwise indicated in new editions.

# Contents

# Chapter 1. Deploy IBM QuickFile as a virtual appliance

If you are deploying IBM® QuickFile, read the installation and configuration topics before you begin the deployment process.

QuickFile is deployed as a virtual appliance. The advantage of using this approach includes the ease of distributing, installing, and configuring the system. After deployment, you have a virtual machine that can be powered on and used to host QuickFile.

A database is required to use the product. The default database is Apache Derby and it requires no special configuration. IBM QuickFile with a Derby database is not supported for a production environment. However, you can use IBM QuickFile with a Derby database for testing. For a production environment, you must use IBM DB2® database or Oracle database.

If you are using QuickFile in a hosted environment, no deployment requirement exists. A hosted environment is also referred to as software as a service (SaaS).

## Understand high availability

High availability is a configuration of two QuickFile instances behind a load balancer.

High availability consists of two QuickFile instances that are controlled by a load balancer. The load balancer is a computer networking method that distributes workload across multiple computers. This method achieves optimal resource utilization and maximizes throughput. The load balancing service is provided by dedicated software or hardware, such as a multilayer switch or a Domain Name System server. QuickFile supports an active and passive high availability configuration. When you configure the load balancer, one instance is configured as the primary instance (active) and one is configured as the secondary instance (passive). The primary is weighted more heavily so it accepts all the traffic unless marked inactive by the load balancer.

**Restriction:** QuickFile does not support sticky sessions or session persistence settings.

Configure the load balancer and identify the primary and secondary instances. In a production environment, the primary instance sends and receives files. If the primary instance is unavailable, the load balancer automatically switches work to the secondary instance.

The following specific behaviors occur as a result of the switch from a primary to a secondary instance:

- If you use the Advanced File Transfer feature, the high availability instances respond in the following way:
  - If the primary instance loses its connection, the file transfer is interrupted. The transfer is available on the secondary instance and displays as paused on that instance. You can resume the file transfer from the secondary instance after you log in.

  - If the primary instance becomes available while the transfer on the secondary instance is in progress, it is interrupted. The status of the transfer on the primary instance displays as paused. After the user logs in, the user can resume the transfer.
- If you use basic file transfer, the instances respond in the following way:
  - If the user sends a transfer and the primary instance loses its connection before the transfer is complete, the primary instance is not available. The user must log in to the secondary instance and resend the file transfer.
  - If the primary instance becomes available, the file transfer that started on the secondary instance completes. The user must restart the primary instance and log in to use it.

# Configuring QuickFile for high availability

Use the information to configure high availability for QuickFile. High availability is two or more QuickFile appliances that share an external database and NFS file system, behind a load balancer. Deploy two OVA files. Then, configure both instances for high availability.

## Before you begin

To configure high availability for QuickFile, both instances must be configured with the same information, identified in the following list:

- An external database that both QuickFile instances share
- An NFS server for file storage that both instances share
- The external IP address and port of the load balancer

The load balancer routes traffic to the primary node. If the primary node goes down, the load balancer switches to the secondary node and routes traffic to it. When the load balancer detects that the primary node is back up, it routes traffic back to the primary node. Use the same properties file for each deployment.

**Important:** When you make configuration changes to QuickFile, you must log on directly to each instance. Do not log on through the load balancer. The same changes must be made to both instances.

## About this task

Complete the following procedure to set up QuickFile instances for high availability:

## Procedure

1. Download the OVA file.
2. Download the database scripts for the OVA.
3. Use database client software, such as dbWiz or Squirrel, to run scripts 0, 1, 2, and 3. The scripts create the database tables and load the default data.
4. On a system that the OVA can access, create a properties file with the configuration of your database instance. Include the NFS configuration and the external IP address and port that is used in the load balancer configuration.
5. Deploy the OVA.
6. Log in to the appliance.
7. Type **Y** to set up the IP address.

8. Type **Y** to set up the DNS.
9. Type **Y** to import the properties file you created.
10. If wanted, change the admin password. This password applies only to this instance. You must change the password of the second instance to keep the two locations in sync.

### Results

The configuration takes a few minutes. Then, QuickFile is available.

## Plan your deployment

A critical decision during the planning phase of your deployment is the type of file system. Plan either a local file system or an NFS implementation. You cannot change from one type of file system to the other after deployment. You must start a new deployment.

During the planning phase of your deployment, you must choose between the following file system types:

- Local file system
- Network file system (NFS)

The type of file system cannot be changed after deployment without risk of files that are not retrievable or removable.

## Preparing to use the IBM DB2 database

You can use the DB2 database in place of the default database when you deploy QuickFile. To use DB2, you create a temporary table space. Then, deploy the software, run the scripts, and create the properties file.

**Restriction:** The properties file is required for the configuration process.

To configure the DB2 database for use with QuickFile, complete the following tasks in the DB2 instance:

- Create a 32-KB system temporary table space
- Create a 32-KB system buffer pool

To configure QuickFile to use DB2, complete the following tasks after you deploy the product:

1. Download the database scripts from the following site: IBM QuickFile Database Scripts.
2. Run the following scripts, in the order that is listed in the following table:

   **Restriction:** You must have system administrator authority for the DB2 instance to run the scripts.

| Script | Description |
|---|---|
| `0_createSchemaObjects.sql` | Creates tables, indexes, and constraints |
| `1_loadDefaultSystemData.sql` | Loads system data records |
| `2_loadDefaultGroupsAndUsers.sql` | Loads group and user support data records |
| `3_loadDefaultConfigurationData_ova.sql` | Loads configuration data records |

3. Customize the properties file to specify that DB2 is being used as the database. See “Customize your deployment with a properties file” on page 8 for instructions.
4. Deploy the product. See “Deploying QuickFile as a virtual appliance” on page 5.

**Tip:** If you do not want to use this database, run the script that is named **`9_dropSchemaObjects.sql`**. It removes all tables, indexes, and QuickFile data. Be sure that you do not need the data before you run this script.

## Support for the Oracle RAC database

QuickFile supports by using Oracle RAC as the QuickFile database. With Oracle RAC, you can scale your database by using multiple servers to distribute query processing across multiple nodes. QuickFile was only tested with the failover feature.

Support for Oracle databases does not include support for the Oracle Exadata platform. The following is an example URL that was used during testing:

```
jdbc:oracle:thin:@(DESCRIPTION= (ADDRESS_LIST=  (LOAD_BALANCE=OFF) (FAILOVER=ON) (ADDRESS=(PROTOCOL=
```

When you are using Oracle RAC, transactions in process at the time of failure are not processed again. Log off and log on to continue working with the system. In some cases, you might be required to restart the browser to recover from Oracle RAC failover.

### Limitations

The following Oracle RAC technologies are not tested or are not supported by QuickFile:

- Load Balancing - The load balancing feature was not tested with QuickFile. If you use this feature and encounter problems, IBM may choose to provide fixes at its own discretion.
- Oracle OCI Type-2 JDBC driver - Because the QuickFile appliance includes the Oracle Thin JDBC Driver, the Oracle OCI Type-2 JDBC Driver is not supported. Any feature of Oracle that requires the OCI driver is not supported.
- Oracle Transparent Application Failover (TAF) - Oracle TAF is a technology that is designed to help applications preserve transactions in the event of a RAC node failure. Oracle TAF requires that the application use the Oracle OCI Type-2 driver. To realize full benefits of TAF, the application must handle Oracle exceptions and use the Oracle OCI API to restart transactions from point of failure. Because QuickFile does not support the OCI Type-2 driver, TAF is not supported.
- Oracle Implicit Connection Cache (ICC) Connection Pool - This connection pool is deprecated by Oracle. Consequently, Oracle ICC connection pool is not supported by QuickFile.
- Oracle Fast Connection Failover (FCF) - Oracle FCF is another technology that is designed to help applications deal with node failure within the Oracle RAC cluster. Like TAF, FCF requires the application to handle the Oracle exception. To achieve connection failover, the application must reconnect inside the catch block after it handles the exception. The QuickFile database access code is database-neutral and does not handle exceptions that are raised by FCF. Therefore, FCF cannot reconnect upon encountering an exception. For these reasons, FCF is not supported by QuickFile.

## Preparing to use the Oracle database

You can use Oracle as the database in place of the default database when you deploy QuickFile. To use Oracle, enable the use of special permissions, run the database scripts, and customize the properties files.

To configure Oracle to use special permissions with QuickFile, run the following commands as user SYS. Replace <*myOracleUserId*> with the user ID for the Oracle connection.

- grant select on `pending_trans$` to <*myOracleUserId*>;
- grant select on `pending_trans$` to <*myOracleUserId*>;
- grant select on `dba_2pc_pending` to <*myOracleUserId*>;
- grant execute on `dbms_xa` to <*myOracleUserId*>;

To configure QuickFile to use the Oracle database, complete the following tasks after you deploy the product:

1. Download the database scripts from the following site: IBM QuickFile Database Scripts.
2. Run the following scripts, in the order that is listed in the following table:

| Script | Description |
|---|---|
| `0_createSchemaObjects.sql` | Creates tables, indexes, and constraints. |
| `1_loadDefaultSystemData.sql` | Loads system data records. |
| `2_loadDefaultGroupsAndUsers.sql` | Loads group and user support data records. |
| `3_loadDefaultConfigurationData_ova.sql` | Loads configuration data records. |

3. Customize the properties file to specify that Oracle is being used as the database. See "Customize your deployment with a properties file" on page 8 for instructions.

**Tip:** If you determine that you do not want to use this database, run the script named **`9_dropSchemaObjects.sql`**. It removes all tables, indexes, and QuickFile data. Be sure that you do not need the data before you run this script.

## Deploying QuickFile as a virtual appliance

To simplify deployment and administration, QuickFile is delivered as a virtual appliance and is deployed to VMware vSphere Hypervisor (ESXi).

### Before you begin

Before deploying QuickFile, install an ESXi hypervisor. ESXi is a bare-metal hypervisor that runs directly on hardware. The VMware Compatibility Guide lists the supported operating systems for ESXi. Be sure that the vSphere version you use for deployment matches the ESXi version.

**Important:** Ensure that your hypervisor is configured to run an NTP server.

To deploy a virtual appliance, you need the VMware vSphere client. The client connects to a hypervisor or group of hypervisors, managed by a virtual center. Go to the VMware website and download the VMware vSphere client. Follow the instructions on the website to install the client.

**Restriction:** QuickFile thin provision deployments require at least 100 GB of available disk space on an ESXi datastore. Thin provision deployments that do not use NFS can grow up to 1.8 TB. If the EXSi datastore has less than 1.8 TB of available storage, you must monitor your QuickFile thin provision deployment for oversubscription. QuickFile thick provision deployments require 1.8 TB of available disk space on an ESXi datastore.

**Restriction:** QuickFile 1.0 deployments require 2 TB of available disk space on an ESXi datastore instead of 1.8 TB.

To deploy a 2-TB virtual appliance, the block size of the datastore must be able to support 2 TB, even with thin-provisioning. To change the block size, delete the datastore and create a new one. The following block sizes are required:

- For ESXi 5.0 and 5.1 with a `VMFS5` datastore, the block size is 1 MB
- For ESX/ESXi 4.1 and ESXi 5.*x* with a `VMFS3` datastore, the block size is 8 MB.

**Important:** The following ports are open on a QuickFile virtual appliance:

| Protocol | Port |
|---|---|
| WebSphere® MQ | 1414 |
| HTTP | 9080 |
| HTTPS | 9443 - This port is only open if SSL is enabled. |

## About this task

After you install the VMware vSphere client, complete the following procedure to begin your deployment:

## Procedure

1. Gather the following information:
   - The IP address to use for the appliance
   - If wanted, the fully qualified host name to use for the appliance

     **CAUTION:**
     **If you specify a host name, it must be registered with your DNS server. Registering the host name allows the remote clients and the appliance to resolve the host name.**
   - IP address of your gateway
   - IP address of your DNS server
   - Subnet mask in CIDR format (for example, 24 is the CIDR format for the subnet 255.255.255.0)
   - IP address of your NTP server. You must specify the same NTP server that is used by the underlying hypervisor.
   - Time zone in POSIX format (for example, `EST5EDT` is US Eastern Time in POSIX format)
   - SMTP server name or IP address of the server to use to send email. The email notifies users when files are sent or received.
   - Password to use to administer the appliance
2. Download the archive named **`QuickFile-1.1.zip`**.
3. Extract the archive. The file named **`QuickFile-1.1.ova`** is extracted. This file contains the QuickFile appliance.

4. Start the ESXi server.
5. To connect to the hypervisor or vCenter, complete the following steps:
   a. Start the VMware vSphere client
   b. Type the host IP address
   c. Type a user name with full access rights and the password
   d. Click **Login**.
6. Choose **File** > **Deploy OVF Template** from the main menu of the vSphere client.
7. When prompted, type the location of the file you extracted.
8. Click **Next** and accept the defaults on the next several pages with the following exceptions:
   - On the Disk Format page, select **Thin Provisioning**
   - On the last page, check **Power on after deployment** and click **Finish**.
9. Wait for the deployment and power on to complete. The process takes several minutes. The OVA file is deployed.
10. Using the vSphere client, go to the **Console** tab to see the QuickFile command line. On this command line, a login prompt is displayed. If not, press Enter.
11. When you are prompted for the login, type `admin` for the user name and `admin` for the password. When you are prompted, provide information that you gathered in step 1 in the following fields.
    - IP address to use for the appliance
    - Subnet mask for the appliance
    - Default gateway for the appliance
12. Confirm the values that you entered.
13. When prompted to set the DNS server, type `Y`, type the DNS server IP address. To specify multiple DNS servers, separate each IP address with a space. Confirm your entry.
14. To change the database to DB2 or Oracle or to specify an NFS file system, upload a properties file. To customize either of these variables, type `Y`. See "Customize your deployment with a properties file" on page 8. Otherwise, type `N`.

    **Note:** The default database is Apache Derby and it requires no special configuration. IBM QuickFile with a Derby database is not supported for a production environment. However, you can use IBM QuickFile with a Derby database for testing. For a production environment, you must use IBM DB2 database or Oracle database.

    When you provide all information, the appliance configures itself. This process takes several minutes. A message is displayed, that the application is available at `http://`*`ip address`*`:9080/quickfile/login.html`. Wait a few minutes before you use the appliance.
15. When prompted to change the administrator password, type the new password.

    **Important:** To protect the system from external access, define a strong password.
16. Start a web browser and type `http://`*`ip address`*`:9080/quickfile/login.html`
17. Log in to QuickFile as the administrator.

**Important:** The default administrator name is `admin` and the password is `admin`. If you changed the password in a previous step, type the new password in this field.

18. Access the Appliance administrative setup pages by clicking **Configuration** from the menu.
19. If you are using the default database, set your time zone on the **Locale** tab. Click **Save**.
20. If you changed the timezone, you are prompted to restart the application. Click **Yes** to restart the appliance.

    **CAUTION:**
    **Do not manipulate the database outside the application. Manipulating the database outside QuickFile threatens the integrity and security of product data.**

## Customize your deployment with a properties file

When you are configuring QuickFile, you can upload a properties file to customize your deployment.

The properties file can customize QuickFile with the following actions:

- Configure a mail server
- Configure use of an external NFS file system
- Change the timezone
- Enable a DB2 or Oracle database in place of the default database
- Configure LDAP in QuickFile
- Enable SSL

You can create more than one properties file to define more than one configuration. To customize a function, change the values of the appropriate properties and save the file.

The properties file must have the following characteristics:

- A text-only file with no hidden return or other characters
- Stored in a location where the computer where you deploy the appliance can access it
- UTF-8 encoded
- Accessible for FTP, SCP, or HTTP

You specify the location of a properties file during deployment, in response to the question:

```
Would you like to upload an IBM QuickFile configuration properties file? (y/n):
```

To change the settings on an existing configuration, upload a new version of the properties file and restart the application.

The following table identifies the configuration properties:

*Table 1. Mail server properties*

| Property | Description | Restart |
|---|---|---|
| `smtp.server` | Host name or IP address for the SMTP server. | yes |
| `smtp.port` | Port number of the SMTP server. | yes |
| `smtp.user` | SMTP user name. | yes |

*Table 1. Mail server properties (continued)*

| Property | Description | Restart |
|---|---|---|
| `smtp.password` | SMTP password. | yes |
| `smtp.secure.mode` | Security mode of the SMTP sessions. Valid values are SSL, TLS, or leave blank for unencrypted sessions. | yes |

*Table 2. Host name properties*

| Property | Description | Restart |
|---|---|---|
| `external.server.host` | External host name or IP address of the appliance. Used with load balancers or VMware proxies. | no |
| `external.server.port` | External port of the appliance. Used with load balancers or VMware proxies. | no |

*Table 3. Server properties*

| Property | Description | Restart |
|---|---|---|
| `dns.servers` | IP addresses for the DNS servers. Multiple addresses are delimited with semicolons. | no |
| `ntp.servers` | IP addresses of NTP server. Only one NTP server is supported. **Important:** Specify the same NTP server that is used by the underlying hypervisor. | no |
| `timezone` | Time zone of the current appliance. | yes |

*Table 4. NFS properties*

| Property | Description | Restart |
|---|---|---|
| `nfs.server` | Host name or IP address for the NFS server. **Important:** Do not change an existing local file system implementation to an NFS implementation. | yes |
| `nfs.directory` | Directory path that is exported from remote system to be mounted as a file system on the appliance. | yes |
| `nfs.reset` | If set to `true`, unmount NFS directory and reset the following DB fields to the local system defaults:<br>• `app.repository.dir`<br>• `app.photos.dir`<br>• `app.email.template.dir`<br>If set to `false`, causes the exported directory to be NFS mounted. | yes |

*Table 5. Database properties*

| Property | Description | Restart |
|---|---|---|
| `db.type` | Database type (DB2 or Oracle). If you use the default Derby database, no database type is required. The application defaults to Derby, unless you define this value. | yes |
| `db.userid` | DB login user ID credentials. | yes |
| `db.password` | DB login credentials - password. | yes |
| `db.db2.server` | DB2 only. Host name or IP address for the database server. | yes |
| `db.db2.port` | DB2 only. Port number for the database server. | yes |
| `db.db2.name` | DB2 only. Database name. | yes |

*Table 5. Database properties (continued)*

| Property | Description | Restart |
|---|---|---|
| db.db2.schema | DB2 only. Schema. | yes |
| db.oracle.url | Oracle only. Connection URL string | yes |

*Table 6. LDAP properties*

| Property | Description | Restart |
|---|---|---|
| ldap.enabled | true = LDAP enabled; false = LDAP disabled. | no |
| ldap.server.host | The host name or IP address of the LDAP server. Text field. Required (no default). | no |
| ldap.server.port | The port number of the LDAP server. Numeric text field. Default = 636. Valid values 1 - 65535. | no |
| ldap.user.base.dn | Parent node where users are stored in the LDAP server. Text field. Required (no default). | no |
| ldap.group.base.dn | Parent node where groups are stored in the LDAP server. Text field. Required (no default). | no |
| ldap.user.search.filter | Search filter for users. Text field. Default is (\|(objectClass=user)<br><br>(objectClass=person)<br><br>(objectClass=inetOrgPerson)<br><br>(objectClass=organizationalPerson)) | no |
| ldap.group.search.filter | Search filter for groups. Text field. Default is (\|(objectClass=group)<br><br>(objectClass=groupOfNames)<br><br>(objectClass=groupOfUniqueNames)) | no |
| ldap.protocol | SSL protocol. Required. Valid values: ldap to create a clear connection to the LDAP server, ldaps to create an SSL connection to the LDAP server. | no |
| ldap.member.attribute | String representing an array of attribute names. Each string specifies the name of an attribute denoting group membership. | no |
| ldap.service.principal | Fully qualified distinguished name of an LDAP user who can search the directory. Text field. Required (no default). | no |
| ldap.service.principal.password | Password of the service principal. Text field. Required (no default). | no |
| ldap.authorized.groups | String representing an array of strings. Each string specifies the DN of an LDAP group that contains users who are authorized to access the QuickFile system. For example: ["cn=Testers,ou=User Groups,ou=QFad,DC=AIXTST,DC=LDAP"] | no |
| ldap.email.attribute | String representing an array of attribute names. Each string specifies the name of an attribute in a user class that identifies an email address. Required. The default value is ["mail","userPrincipalName", "email","emailAddress"]. | no |

*Table 7. Application properties*

| Property | Description | Restart |
|---|---|---|
| sys.admin.email | Email address of the system administrator. | no |

*Table 7. Application properties (continued)*

| Property | Description | Restart |
|---|---|---|
| app.sender.email | The "no-reply" account email address. This email address is used for email notifications that are sent by QuickFile. | no |
| sessioninvalidationtimeout | Set how long a session can be idle before it is closed. Set the value 2 - 1440 minutes. The default value of 30 minutes is used if no value is provided. It is also used if an invalid value, such as a number outside the valid range or a non-numeric value, is provided. | yes |
| ssl.enabled | Security enhanced with SSL. The following are valid values:<br>• true = SSL connection enabled<br>• false = SSL connection disabled | yes |

**Remember:** Any line that begins with # is treated as a comment.

### Sample properties file

The following sample properties file specifies the location of an NFS file system and the location of a DB2 database. Oracle database information is commented out. Define your properties file with the values appropriate to your deployment.

```
nfs.server=myserver.example.org
nfs.directory=/localhome/bsmith/NFSdatadirectory
nfs.reset=false

db.type=DB2
db.userid=bsmith
db.password=password
db.db2.server=myDB2server.example.org
db.db2.port=50001
db.db2.name=QUICKFILE
db.db2.schema=QUICKFILE

#db.type=Oracle
#db.userid=cjones
#db.password=password2
#db.oracle.url=jdbc:oracle:thin:@myOracleDBserver.example.org:1522/DEV11R1
```

To specify an NFS server, remove the # at the beginning of each line in the first paragraph. Specify your NFS server name along with the directory where the NFS data is to be stored. If you do not want to specify an NFS server, comment out these lines with the # at the beginning of each line.

To specify an Oracle database, comment out the DB2 lines. Then, uncomment the lines for the Oracle database, and provide the values that pertain to your Oracle database.

## Tuning the environment

Tune your environment to improve performance according to the type of transactions you support and your business requirements. Tune the behavior for certain functions by changing values in the properties file.

Monitor the performance of your system and the characteristics of files transferred. To tune a function, change the values of the appropriate properties and save the file.

A properties file must be a text-only file with no hidden return or other characters. It must be stored in a location where the computer where you deploy the appliance can access it. It must be UTF-8 encoded and accessible for FTP, SCP, or HTTP. You specify the location of a properties file during deployment.

**Remember:** Any line that begins with # is treated as a comment.

The following table identifies the configuration properties:

| Property | Description |
|---|---|
| `channel.http.inbound.readtimeout` | How many seconds the HTTP transport channel waits for a read request to complete on a socket after the first read occurs. The read might occur in the body of the read request, such as a POST. It might occur in the headers, if all headers are not read in the first read. Default is 60 seconds. |
| `channel.http.inbound.writetimeout` | How many seconds the HTTP transport channel waits for each portion of the response data to be transmitted. This timeout occurs only in situations where the writes are lagging behind new requests. This situation might occur when a client has a low data rate or the network interface card (NIC) is saturated with I/O traffic. If clients require more than 300 seconds to receive data that is being written, change the value that is specified for this parameter.<br><br>Some clients require more than 300 seconds to receive data that is sent to them. To ensure that they are able to obtain all data, change the value for this parameter. Make sure that the length is sufficient for all data to be received. If you change the value of this setting, make sure that the new value still protects the server from malicious clients. Default is 60 seconds. |
| `channel.http.inbound.persistenttimeout` | How many seconds that the HTTP transport channel allows a socket to remain idle between requests. Default is 30 seconds |

# Enabling event purge

Enable event purge to maintain performance of your system.

## About this task

Event purging may be suspended. To avoid declining performance, resume **PurgeEvents**:

## Procedure

1. From the **Administration** menu, select **Policies** and click the **Schedules** tab.
2. Click **Show all tasks**. If the **PurgeEvents** task is in **Suspended** status, you must resume the schedule.

3. To initiate purging of system events, select **Resume** in the selection box for **PurgeEvents**. The default is for the task to run weekly on Sunday at midnight to purge events older than 30 days. The label changes to **Scheduled**.

### What to do next

See "Configuring event purge" on page 67 for more options.

## Branding the product to display your company information

You can customize QuickFile to display your company information on QuickFile pages and email notifications.

So that your users know who is hosting their QuickFile file transfer application, you can substitute the IBM logo and standard colors and messaging with ones that are more identified with your company. You can customize the following elements:

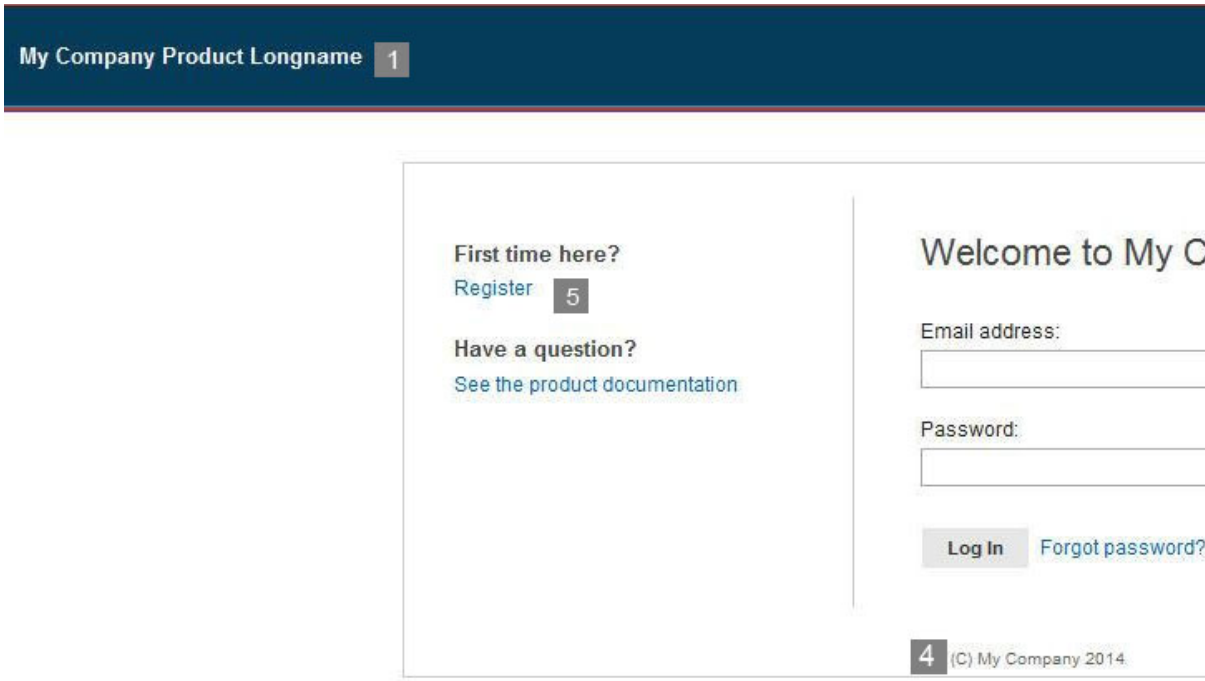
- For the user interface:
  - Company name
  - Welcome message
  - Logo
  - Colors
  - Copyright statement
- For the email notifications:
  - Company name
  - Logo and size of logo
  - Colors
  - Copyright statement

### Properties for branding the user interface

Specify custom values for properties to define elements on the Login page and the Welcome page.

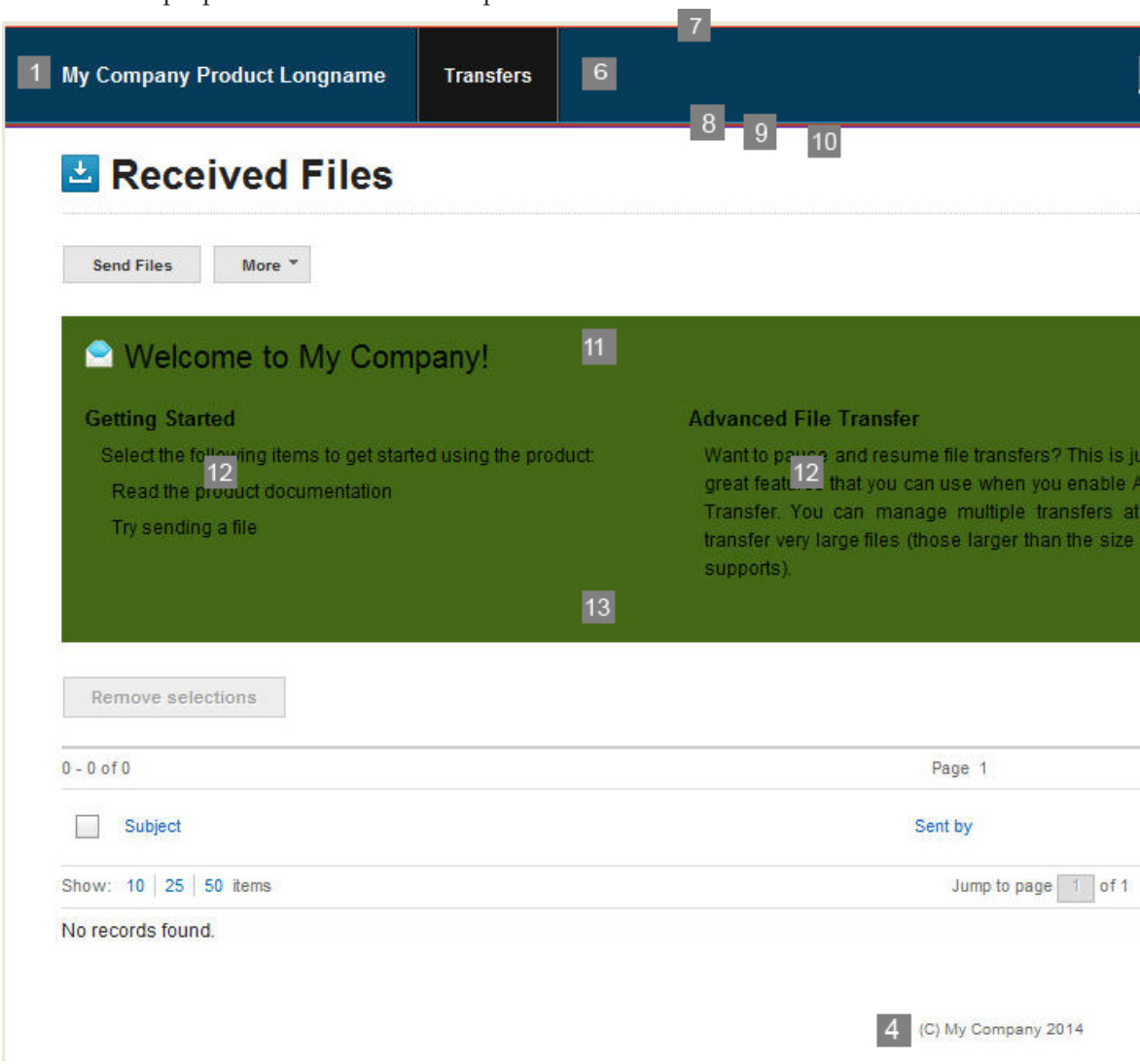
## Login page

The following graphic shows the parts of the interface on the Login page with labels for the properties that define each part:



## Welcome page

The following graphic shows the parts of the interface on the Welcome page with labels for the properties that define each part:




**1**
**productLongName**
Full name of the product to display in the interface, for example, IBM QuickFile

**2**
**bannerLogoImage**
Graphic that displays in the banner on each page. The banner logo image can be up to 60 pixels high and 300 pixels wide. Specify the name of the graphic file for this value. Graphic file types can be .jpg, .gif, or .png

**3**
**welcomeLogoImage**
Graphic to display as the company logo. The welcome logo image can be up to 60 pixels high and 200 pixels wide. Specify the name of the graphic file for this value. Graphic file types can be .jpg, .gif, or .png

**4**
**copyright**
Text to display in the copyright property, for example, (C) COPYRIGHT Zeta Hospital 2013. This text appears on every page of the interface including the Welcome page (11).

**5**
**showRegistration**
Determines whether the registration link is displayed on the login page. Valid values are true to display the registration link or false to remove the registration link from the login page. Type the value for this field, true, or false, in lowercase characters (12).

**6**
**mainBannerColor**
Color that is used on the banner. Use either a hex value, such as #ED7818 or a color name, such as blue

**7**
**mainBannerTopBorderColor**
Color that is used on the top border of the banner. Use either a hex value, such as #ED7818 or a color name, such as red.

**8**
**mainBannerBottomBorderColor**
Color that is used on the bottom border of the banner. Use either a hex value, such as #ED7818 or a color name, such as green.

**9**
**subBannerColor**
Color that is used on the sub banner, the small banner under the main banner. Use either a hex value, such as #ED7818 or a color name, such as green.

**10**
**subBannerBottomBorderColor**
Color that is used on the bottom border of the small banner that is displayed under the main banner. Use either a hex value, such as #ED7818 or a color name, such as green.

**11**
**welcomeMessage**
Welcome message that is displayed on the login page and Welcome banner, for example, Welcome to My Company

**12**
**welcomeDividerTextColor**
Color of the text on the Welcome banner and initially displayed on the Transfers listing page. Use either a hex value, such as #ED7818 or a color name, such as green

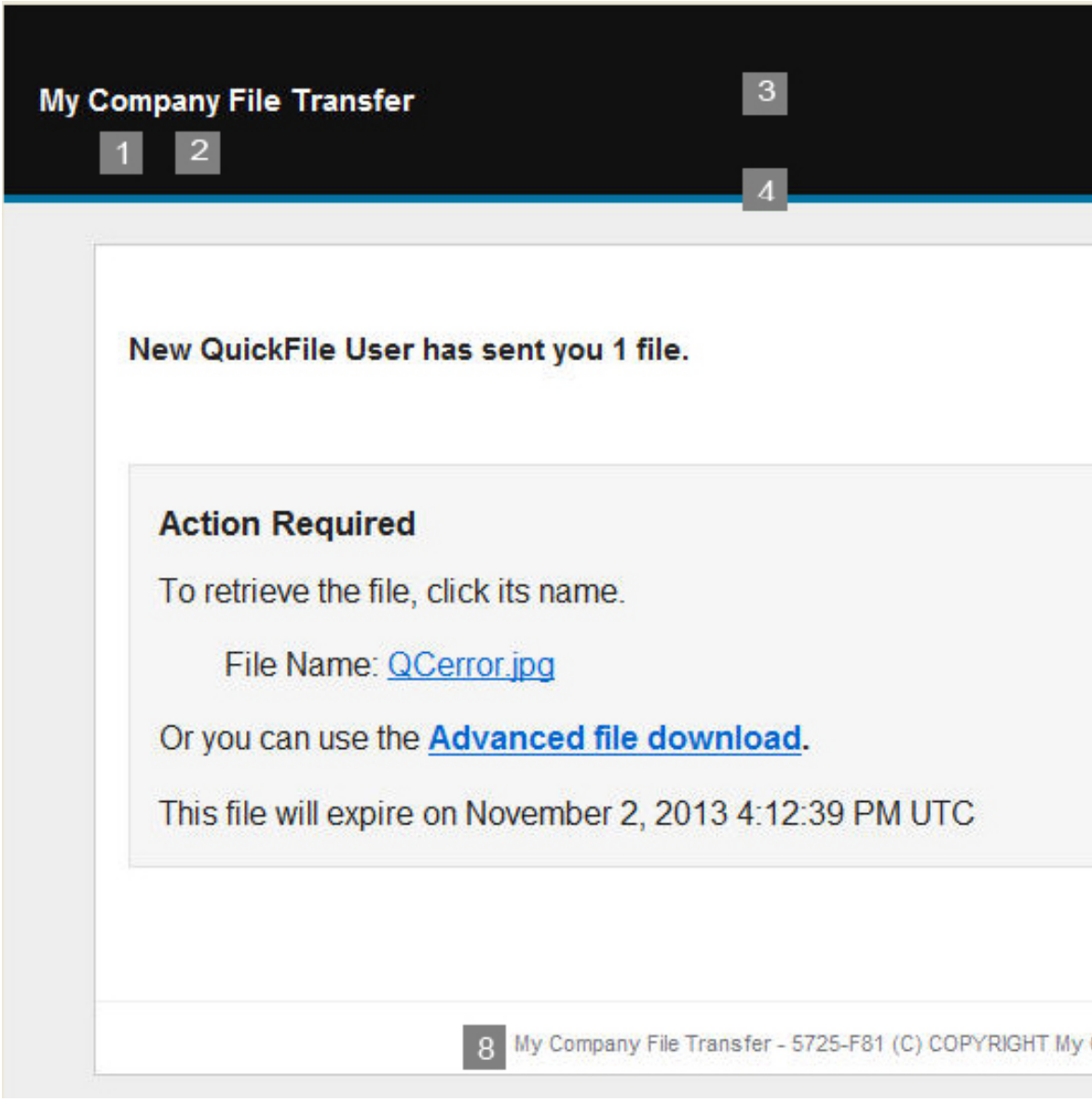
**13**
**welcomeDividerColor**
The background color on either the Welcome banner or the page divider that is displayed on the file listings page. Use either a hex value, such as #ED7818 or a color name, such as green

## Properties for branding email notifications

Specify custom values for properties to define elements on the email notifications that users receive for registration confirmation, transfer status, and pending expirations.

### Email notification

The following graphic shows the parts of the interface on the email notification with labels for the properties that define each part:




**1**
**companyName**
Company name to display in the email notification. For example, `My Company File Transfer`.

**2**
**companyNameColor**
Font color to use for the company name. Specify colors as HTML color codes, such as `#E01B6A`, or as a color name, for example, `white`.

**3**
**bannerBackgroundColor**
The background color of the banner.

**4**
**subBannerBackgroundColor**
The background color of the banner.

**5**
**logoHeight**
Height dimension for the company logo, in pixels.

**6**
**companyLogo**
Graphic file, in jpg format, for the banner of the email. The default value is `company.jpg`. The maximum size that is allowed is 25K.

**7**
**logoWidth**
Width dimension for the company logo, in pixels.

**8**
**copyright**
The copyright information that is shown in the email footer.

## Branding the user interface for your users

Create a properties file with custom values to modify the user interface for your users. Upload it to your QuickFile server to initiate the changes

### About this task

To customize each QuickFile page with your company information:

### Procedure

1. Create a text file that is named `ui-branding_en_US.properties`.
2. Copy the following sample code into the file that you created.

```
productLongName=My Company Product Longname
showRegistration=true
welcomeMessage=Welcome to My Company!
bannerLogoImage=bannerLogoImage.jpg
welcomeLogoImage=welcomeLogoImage.jpg
welcomeDividerTextColor=#010802
welcomeDividerColor=#446816
mainBannerColor=#053C5A
mainBannerTopBorderColor=#ED452B
mainBannerBottomBorder=#90717A
subBannerColor=#B23D2E
subBannerBottomBorderColor=#5B2EAD
copyright=(C) My Company 2014
```

3. Change the values of the properties to your custom values. See "Properties for branding the user interface" on page 13.
4. If you do not want to customize a property, set the property value to empty. For example, to use the default color, black, for the Welcome divider color, set:

```
welcomeDividerColor=
```

   To remove all branding from the page, set all values in `ui-branding_en_US.properties` to empty.
5. Save the file and your graphics files to a location on your local drive.

6. Log in to QuickFile as an administrator.
7. From the **Welcome** page, click **Transfers** > **Sent**.
8. On the Sent Files page, click **Send Files**.
9. In the **Send to** field, type a recipient name. Use the format: `username@domainname`, for example `myuser@company.com`.

   **Tip:** The recipient name is not used. The files are sent to an internal location when you type `branding` as the Subject value.
10. In the **Subject** field, type `branding`.
11. Attach the `.properties` file that you created, and the graphic files for the welcome logo and the banner logo.
12. Click **Send**. The file that you created and logo graphic files are sent to the server to define the product pages branding. After the `.properties` files and graphic files are sent to the server, the customization changes are in effect when the server processes the files.

## Branding the email notifications for your users

Create a properties file with custom values to modify the email notifications users receive for registration confirmation, transfer status, and pending expirations. Upload it to your QuickFile server to initiate the changes.

### About this task

To brand the email notifications with your company information:

### Procedure

1. Create a text file that is named `email_defaults_en_US.properties`.
2. Copy the following sample code into the file that you created.

```
companyName=My Company File Transfer
companyNameColor=#ffffff
bannerBackgroundColor=#111111
subBannerBackgroundColor=#0075A3
companyLogo=companyLogo.jpg
logoHeight=68
logoWidth=143
copyright=5725-F81 (C) COPYRIGHT My Company Name Corp. 1999
```

3. Change the values of the properties to your custom values. See “Properties for branding email notifications” on page 17.
4. To use the default value for a property, set the value to empty. For example, to use the default color, black, for the company name, set:

   ```
   companyNameColor=
   ```

   To remove all branding from the email notifications, set all values in `email_defaults_en_US.properties` to empty.
5. Save the file and your graphics files to a location on your local drive.
6. Log in to QuickFile as an administrator.
7. From the **Welcome** page, click **Transfers** > **Sent**.
8. On the Sent Files page, click **Send Files**.
9. In the **Send to** field, type a recipient name. Use the format: `username@domainname`, for example `myuser@company.com`.

   **Tip:** The recipient name is not used. The files are sent to an internal location when you type `branding` as the Subject value.

10. In the **Subject** field, type `branding`.
11. Attach the `.properties` files that you created, and the graphic file for the logo.
12. Click **Send**. The file that you created and logo graphic file are sent to the server to define the email notification branding. After the `.properties` file and graphic file are sent to the server, the customization changes are in effect when the server processes the files.

## Viewing the license

The license is downloaded as part of the deployment. If your company requires that the license is reviewed before you use the application, first deploy the application. Then, use the get license utility to review the license.

### Before you begin

**Attention:** A license is installed when you deploy the application. To view the license content, you must first deploy the application.

### About this task

To download and view the license information from the console:

### Procedure

1. Type `wizard getLicense.xml`. The wizard packages the license files into a compressed file.
2. You can then send the file to another host where you uncompress and view the license files.
3. You can also print the license files.

## Upgrading to QuickFile 1.1 as a virtual appliance

If you deploy QuickFile as a virtual appliance, upgrade the product whenever a new version is released. If you use QuickFile in a hosted (SaaS) environment, you are not required to upgrade the appliance.

### Before you begin

To successfully upgrade QuickFile to version 1.1, your virtual appliance must be configured for a minimum of 8 GB of memory. Verify the available memory that is configured for your QuickFile instance before proceeding. For more information, see the VMware documentation.

Download the firmware upgrade file from the IBM Fix Central website. The firmware upgrade file has an extension of `vcrypt2`. If you are deploying QuickFile with an external database, download the 1.1.0.0 QuickFile SQL upgrade file for your database (Oracle or DB2). Copy the firmware upgrade file and the database upgrade script to an FTP, SCP, or HTTP server that is accessible from QuickFile.

### About this task

To upgrade a virtual appliance, use the VMware infrastructure client to connect to a hypervisor or group of hypervisors (managed by a virtual center).

Complete the following procedure to upgrade your deployment:

## Procedure

1. Shut down all connections to the server where QuickFile is running.

   **CAUTION:**
   **Before you upgrade the QuickFile database, you must stop connections to avoid instability.**

2. Run the following command from your QuickFile command-line console to retrieve the firmware upgrade file from the server where you downloaded the file:

| Command name | Variable Description | Examples |
|---|---|---|
| `file get` *URL filename* | • *URL* is the host, path, and file name for the firmware upgrade file.<br>• *filename* is the name to save the file as on the appliance. This file name can be any valid file name, with no path (for example, fw) | FTP<br>`file get ftp://user1@dallas.ibm.com:/downloads/upgrade/091112.vcrypt2 fw`<br>SCP:<br>`file get scp://user1@dallas.ibm.com:/downloads/upgrade/091112.vcrypt2 fw`<br>HTTP:<br>`file get http://user1@dallas.ibm.com:/downloads/upgrade/091112.vcrypt2 fw` |

   **Remember:** If you turn off the appliance, the upgrade file is deleted. Upgrade the appliance before you turn off the appliance.

3. Take a VM snapshot of the QuickFile server. This snapshot can be used to restore the instance if the firmware upgrade fails and the automatic rollback that occurs after a failed upgrade also fails. For more information, see the VMware documentation.

   **Important:** If you deployed a version 1.0.0.0 `.ova` file, you cannot take a VM snapshot because VMware generates an error.

4. If you are using an external Oracle or DB2 database, back up the QuickFile database.

   **Important:** If the upgrade fails, you must have a backup of your database to recover. For more information, see the DBMS documentation.

5. If you are using an external Oracle or DB2 database, edit the QuickFile 1.1.0.0 SQL script, `1.1.0.0.sql`, and change the schema to the schema that the database is using.

6. If you are using an external Oracle or DB2 database, upgrade the database by running the edited QuickFile 1.1.0.0 SQL script on the database server. For more information, see the DBMS documentation.

   **Important:** If you perform the following steps before you complete steps 5 and 6, the upgrade will fail.

7. Reorg all QuickFile tables. For more information, see the DBMS documentation.

8. Run the following command from your console to upgrade QuickFile:

| Command name | Variable Description | Example |
|---|---|---|
| `firmware upgrade filename` | *filename* - the name that is used in the file get command. | `firmware upgrade fw` |

9. Wait for the firmware upgrade command to finish. The command might take a long time. The appliance restarts when the upgrade completes.

   **Restriction:**

   After the **firmware upgrade** command completes, the appliance automatically restarts. When the appliance starts again, the **show version** command shows that the appliance is running on the new version. However, sometimes the **firmware upgrade** command completes successfully but the appliance does not automatically restart. If you are using an SSH console (for example, putty), the console closes. To verify that the appliance restarted and that the upgrade is applied, do the following after logging in to the appliance console after an upgrade:

   a. Issue a **show version** command on the console.
   b. Verify that the version displayed matches the upgrade version.
   c. If the version displayed is still the old version, issue a **device restart** command to manually restart the appliance.

10. When the appliance restarts, log in to the console with administrative credentials.
11. Follow the prompts to complete the startup process. To use the current settings, type `N` when you are prompted to modify properties. See "Customize your deployment with a properties file" on page 8 for instructions on changing properties.

## What to do next

If the upgrade is unsuccessful, the appliance automatically rolls back the firmware upgrade and restores the original firmware version. If you are using an external Oracle or DB2 database, you must manually restore the database to the original version from the backup in step 4.

To determine the reason for the failure, export the QuickFile log files by running the platform `must-gather` command from the QuickFile command-line console. Copy the log files to a server so that they can be sent to IBM Support for review.

To collect the logs, run the following command:

```
platform must-gather logs.tgz
```

To copy the logs to another server, run the file put command. You can use FTP or SCP, but not HTTP:

```
file put logs.tgz ftp://user1@dallas.ibm.com:/uploads/logs.tgz
file put logs.tgz scp://user1@dallas.ibm.com:/uploads/logs.tgz
```

Restart the appliance with the device restart command to restore operation:

```
device restart
```

If the appliance does not start after the automatic firmware rollback, you must manually restore the appliance from the VM snapshot.

# Upgrading QuickFile with an iFix

If you are using QuickFile in a hosted (SaaS) environment, you are not required to upgrade the appliance. If you are deploying the appliance, you must upgrade the product whenever a new version is released to get the latest improvements.

## Before you begin

Download the upgrade file from the IBM Fix Central website. Enter QuickFile into Product Search. Copy the upgrade file to a server that is accessible from QuickFile. To be accessible, the upgrade file is on a system that the QuickFile instance can access and available using FTP, SCP, or HTTP.

## About this task

To upgrade a virtual appliance, use the VMware infrastructure client to connect to a hypervisor or group of hypervisors (managed by a virtual center).

Complete the following procedure to upgrade your deployment.

## Procedure

1. Run the following command from your QuickFile console to retrieve the upgrade file from your server:

| Command name | Variable Description | Examples |
|---|---|---|
| `file get URL filename` | • *URL* is the server path and file name for the upgrade<br>• *filename* is the name to save the file as. | FTP<br>`file get ftp://user1@dallas.ibm.com:/downloads/upgrade/091112.vcrypt2 fw`<br>SCP:<br>`file get scp://user1@dallas.ibm.com:/downloads/upgrade/091112.vcrypt2 fw`<br>HTTP:<br>`file get http://user1@dallas.ibm.com:/downloads/upgrade/091112.vcrypt2 fw` |

   **Attention:** If you turn off the appliance, the upgrade file is deleted. Upgrade the appliance before you turn off the appliance.

2. After you retrieve the file, run the following command from your console to upgrade:QuickFile

| Command name | Variable Description | Example |
|---|---|---|
| `firmware upgrade filename` | • *filename* - the name that is used in the file get command. | `firmware upgrade fw` |

3. The appliance restarts.

   **Restriction:**

   After the **`firmware upgrade`** command completes, the appliance automatically restarts. When the appliance starts again, the **`show version`** command shows

that the appliance is running on the new version. However, sometimes the **firmware upgrade** command completes successfully but the appliance does not automatically restart. If you are using an SSH console (for example, putty), the console closes. To verify that the appliance restarted and that the upgrade is applied, do the following after logging in to the appliance console after an upgrade:

a. Issue a **show version** command on the console.
b. Verify that the version displayed matches the upgrade version.
c. If the version displayed is still the old version, issue a **device restart** command to manually restart the appliance.

4. When the appliance restarts, log in to the console.
5. Follow the prompts to complete the startup process. To use the current settings, type `N` when you are prompted to modify properties. To accept a property that changed in the properties file, type `Y`. See "Customize your deployment with a properties file" on page 8 for instructions on changing properties.

# Chapter 2. Administration questions

As administrator, you are responsible for many tasks. Tasks include adding users and groups, configuring security for users, and defining when files are purged from the server.

Use the following table to answer questions you have about administrative tasks:

| Question | Answer |
|---|---|
| How do I make sure that my server has disk space available to add more files? | To make sure that your server has the space available to upload files for transferring, define a schedule for purging files and system events.<br><br>You define the conditions under which files are removed from the server, including files that are abandoned during upload. From the **Administration** menu, select **Policies**. Click the **Schedules** tab, then **Purge** to set when files are deleted from the system.<br><br>Select **PurgeEvents** to set when system events are deleted from the system. |
| Can I change how many times a user can attempt a login before the user is locked out? | Yes. You can change how many times a user can log in incorrectly before the user is locked out. Click **Administration** from the menu and select **Policies**. Click the **Password** tab to set password options. |
| Can I control what policies are required for user passwords? | Yes, you can set the strength requirements, how long a password is valid, how frequently a password can be changed, and the characters required. Click **Administration** from the menu and select **Policies**. Click the **Password** tab to set password options. |
| Can I configure the product to work with Sterling Secure Proxy? | Yes. This product works behind Sterling Secure Proxy. In order for the two products to work together, configure the network configuration to support Sterling Secure Proxy. See “Protecting QuickFile with Sterling Secure Proxy” on page 32 |
| Can anyone decrypt the appliance disk? | No. Direct access to the virtual disk in the appliance is not available. Decryption of the content is not possible. |
| Can I use the CMIS PI to extract a file that belongs to someone else? | Yes. You can use the CMIS API to extract files. You might want to use the CMIS API to archive files if you do not use FileNet. |
| When are files archived? | If you configured archiving, files are queued for archiving after the file is uploaded. Files queued for archiving are processed on a first in first out basis. |

| Question | Answer |
| --- | --- |
| Are files deleted after they are archived? | No. A copy of the file is moved to the archive queue. The original file is processed by QuickFile. If you configure the purge maintenance task, the files are deleted on the defined schedule. |
| If NFS is not encrypted, is the environment no longer secure? | Correct. To maintain a secure environment, encrypt the NFS hardware. |
| Can I change the default user name and password that is used to connect to WebSphere MQ? | You cannot change the default user name and password. |
| Can I set up File Download Notification to remove the register link? | Yes. If you configure the file transfer policy and restrict users from inviting other users to register, the registration option is removed from the login page. See<br>• "Defining file transfer restrictions" on page 72<br>• "Defining users who are allowed to send registration invitations" on page 73 |
| How many times can a user download a file? | A user can download a file as many times as needed until the file download expires. "Policies for file transfer expiration and file size" on page 71 |
| When and how often are events purged? | The **PurgeEvents** task must first be resumed so that it is scheduled. The default is for the task to run weekly on Sunday at midnight to purge events older than 30 days. You can set the interval and schedule for **PurgeEvents** to run, based on your business needs. See "Configuring event purge" on page 67. |
| Why is my system accumulating such a large number of events? | The **PurgeEvents** task must first be resumed so that it is scheduled. The number of transactions in your system that cause events might be greater than average. Change the settings for **PurgeEvents**. See:<br>• "Enabling event purge" on page 12<br>• "Configuring event purge" on page 67 |

# Chapter 3. Use IBM Sterling Control Center to track QuickFile transfer events

IBM Sterling Control Center can be used to monitor business activities for QuickFile.

QuickFile is a centralized monitoring and management system that gives operations personnel the capability to continuously monitor business activities for IBM Sterling Connect:Direct®, IBM Sterling Connect:Direct File Agent, IBM Sterling Connect:Enterprise®, IBM Sterling Connect:Enterprise Gateway, IBM Sterling B2B Integrator, QuickFile and many FTP servers, across the enterprise.

Sterling Control Center supports the following events from QuickFile

- Storage of files
- User and groups events
- Messaging for exception items
- Events regarding the appliance
- SSL configuration

# Chapter 4. Configure or modify application settings

Configuration options are available to control the setup of QuickFile. Many of the setup options are defined when you deploy the product. Use the Configuration options to modify or add new settings.

As needed, change the configuration of QuickFile. You can change the configuration of QuickFile in the following areas:

- **Network** - change the basic settings of the network, including the network or DNS address or the host name (fully qualified domain name - FQDN). Check the basic settings after you deploy the product.
- If you have a firewall, change the advanced network settings. You can also identify a user on a specific email domain as an internal user.
- **Locale** - configure the NTP server addresses, change the time zone for the server, or change the server locale.
- **System** - identify how long to wait after a session is idle before it is timed out and the user is logged off. The default is 30 minutes. The maximum value is 1440 minutes or 24 hours.
- **Power** - shuts down or restarts QuickFile.
- **ICAP server**- configure the ICAP server to use for antivirus scanning and data loss prevention (DLP)
- **LDAP** - use this option to configure LDAP.
- **Archiving** - enables archiving and configures IBM FileNet®.
- **SSL** - enables SSL authentication.

## When to configure network options

Network options are defined when you deploy the product. View the basic network options after the installation to validate the settings. If necessary, modify the basic network values. For certain network environments, such as the presence of a firewall or the identifying internal users, configure advanced network settings.

- Use the procedure that is called “Setting basic network configuration options” to validate the network address that is defined for the installation. You can also disable the Ethernet connection.
- Use the procedure that is called “Setting basic network configuration options” to configure network requirements specific to your environment. Options include adding or removing a DNS server definition or defining the domain where internal users are stored. In addition, define an SMTP mail server, modify the mail server definition, or configure support for a firewall.

If you change the mail domain that is used for the network, all users on the new domain are designated as internal users. If you remove a mail domain from the network definition, all users on the domain you removed are defined as external users.

### Setting basic network configuration options

Network settings are first set up when the product is installed. After you install QuickFile, use this procedure to validate basic network settings and change them as needed.

### Before you begin

To view and change basic network settings:

### Procedure

1. Click **Configuration** from the menu.
2. On the **Network** tab, click **Network Addresses** to display the address options.
3. To modify an Ethernet interface, complete the following steps:
   a. Enable **eth0** to enable the Ethernet interface.
   b. Type the IP address for the Ethernet interface in the **IP Address** field.
   c. Enter the appropriate **Mask** value in CIDR format.
   d. Type the **Default gateway** address for the interface.
4. To disable an Ethernet interface, disable the box next to its name.
5. To add a domain name DNS server address, click **Click to add**, type the DNS name, and press Enter.
6. To delete a DNS server, click the **x**.
7. To enable the host name that is defined for the network, complete the following steps:
   a. Click **Host Names** to display the host name option.
   b. Type the host name in the **Hostname** field.
8. To configure the NTP server and the time zone for the server, complete the following steps:
   a. Click the **Locale** tab.
   b. To add an NTP server address, click **Click to add** and type a new address.
   c. To delete an NTP server address definition, click the **x** next to its name.
   d. To change the time zone for the server, select the time zone to use, from the list.
9. Click **Save**.

## Configuring advanced network options to define internal users

Configure advanced network settings to prepare specific environments. Set the domains where users are stored in addition to the address set at installation. Configure the email domain names that are used to identify internal users. Until you designate an email domain, all users are created as external users. Define the public facing network options to configure a firewall.

### Before you begin

To view and change network settings for environment requirements, complete the following steps:

### Procedure

1. Click **Configuration** from the menu.
2. If necessary, click the **Network** tab.
3. To define the mail domains where internal users are stored, complete the following steps:
   a. Click **Mail Domains** to display the mail domain options.
   b. To add an internal email domain, click **Click to add**.

c. Type the mail domain where internal users are stored and press **Enter**.

**Remember:** If you change the mail domain that is used for the network, all users on the new domain and all sub-domains are designated as internal users. If you remove a mail domain from the network definition, all users on the domain you removed (and all sub-domains) are defined as external users.

4. To enable security, complete the following steps:
   a. Select **SSL** or **Start TLS** from the **Security** field.
   b. Add the certificate for the SMTP server to the truststore.
5. To change the SMTP mail server, complete the following steps:
   a. Click **Mail Servers**.
   b. Type a server name in the **SMTP Server Name** field and a port in the **SMPT Server Port** field.
   c. To enable security, select **SSL or Start TLS** in the **Security** field. Add the certificate for the SMTP server to the truststore.
6. To authenticate access to the SMTP server, click **Use authentication credentials with smtp server**, then supply the Authorized user name and Authorized password credentials.
7. To configure support for a firewall, select from the following choices:
   - **Use a host name (fully qualified domain name - FQDN)** - Type the **Host name** to use to connect to QuickFile
   - **Use a public-facing domain name (FQDN) or IP address** - Type the **Host name** to use to connect to QuickFile and **Port number**. For example, if you configure a load balancer and SSL, set the port value to 9443. For a unsecure load balancer, define the port as 9080. You can specify other port numbers according to your network architecture.
8. Click **Save**.

**Restriction:** You cannot change a user from an internal user to an external one. To change a user from an internal user to an external user, delete the user account. Then, ask the user to register again. By default, users are defined as external

## Setting public-facing port in a cluster

When QuickFile is deployed behind a load balancer, configure QuickFile to use the load balancer public-facing host name and port on generated email links.

### About this task

The external public-facing port is the public entry to QuickFile. A typical configuration is to put a firewall in front of the load balancer and open that specific port only. You can specify port numbers according to your network architecture.

### Procedure

1. From the **Administration** menu, click **Configuration**.
2. Click the **Network** tab.
3. To configure an external port, select the following choice:
   - **Use a public-facing domain name (FQDN) or IP address** - Type the **Host name** to use to connect to QuickFile and **Port number**.

**Restriction:** When QuickFile is deployed behind a load balancer, clients connect to QuickFile by using the load balancer public-facing host and port number. However, QuickFile has two ports, one for HTTP (9080) and another for HTTPS (9443). Configure the load balancer so that requests to the public-facing port are forwarded as follows:

- To QuickFile port 9080 when the request scheme is HTTP
- To QuickFile port 9443 when the request scheme is HTTPS

## Protecting QuickFile with Sterling Secure Proxy

You can use IBM Sterling Secure Proxy to protect QuickFile in the internal network.

### Before you begin

Configure an HTTP configuration in Sterling Secure Proxy. For more information, see the Sterling Secure Proxy information center.

**Important:** The inbound and outbound HTTP connections can be secure or unsecure, but they must match. If the inbound netmap connection is secure, the outbound netmap connection to QuickFile must also be secure.

Complete the following procedure to configure QuickFile to work with Sterling Secure Proxy:

### Procedure

1. Click **Configuration** from the menu.
2. If necessary, click the **Network** tab.
3. To configure the product to support Sterling Secure Proxy, complete the following steps:
   - Type the host name or IP address of the Sterling Secure Proxy HTTP adapter in the public-facing **Hostname** field.
   - Type the **Port number** of the Sterling Secure Proxy HTTP adapter for this host name.
4. Click **Save**.

   **Important:** If you configured QuickFile to use a self-signed certificate for SSL, you must export the root certificate. Configure the Sterling Secure Proxy HTTP netmap with this certificate. For more information, see the Sterling Secure Proxy information center.

## Solve network issues

Solve network issues that are identified by users and how each issue was resolved.

*Table 8. Network issues*

| Issue | Solution |
|---|---|
| While a user was testing the appliance, the user incorrectly set up the network. The network had errors so I was unable to log in to correct the problem.<br><br>Is there a command to reset the appliance so I can correct the setup? | In the console view of the appliance, run the setup wizard again by entering the following command on the command line:<br><br>**wizard startup.xml**<br><br>Reset just networking by entering the following command:<br><br>**netif set eth0 IPAddress=** *youripaddress***DefaultGateway=***yourdefaultgateway*Substitute your IP address for *youripaddress* and your gateway address for *yourdefaultgateway*. |

## Network configuration field definitions

Define the following fields on the **Network** tab of the Configuration settings to configure basic and advanced network settings:

| Field Name | Description |
|---|---|
| Ethernet interface (eth*x*) | The Ethernet interface that is defined. One Ethernet interface (eth0) is required. Only one Ethernet interface is supported. |
| IP Address | The IP address or mask of the Ethernet interface. Required. |
| Mask | The subnet mask for this IP address. It must be in classless inter-domain routing notation. (CIDR), a means of specifying IP addresses and their routing prefix. It provides the decimal number of leading bits of the routing prefix. For example: 24. Required. |
| Default gateway | The default gateway address for the Ethernet interface. Required. |
| DNS Server address | The address of the DNS server. |
| Internal Email Domains | The domain name servers (DNS) for the appliance. At least 1 domain is required. |
| SMTP Server Name | The SMTP or mail server to use to route email for the appliance. Required. |
| SMTP Server Port | The SMTP or mail server port to use to route email. Required. |
| Security | Security used by the SMTP server: Valid values are None, SSL, or Start TLS. |
| User authentication credentials with smtp server | Enables the use of authentication credentials with the SMTP server |
| Authorized username | A user name with authorization to access the SMTP server. Optional. |
| Authorized password | The password for the user who is authorized to access the SMTP server. Required if **Authorized user name** is specified. |

| Field Name | Description |
| --- | --- |
| Use a host name (fully qualified domain name - FQDN) | Enable this option only when a host name is assigned to the QuickFile appliance, and the host name to IP address mapping is added to DNS.<br><br>When this field is enabled, you can access QuickFile by using the fully qualified distinguished name. The distinguished name is easier to remember than an IP address. If you set this field to a host name that cannot be resolved by the appliance DNS, an error occurs. |
| Host name | DNS host name of the QuickFile appliance.<br><br>If no host name is assigned, the field displays the IP address of the first network that is configured. |
| Use a public-facing domain name (FQDN) or IP address | Check this field when QuickFile is deployed behind a reverse proxy or load balancer. If this option is enabled, type the public-facing, fully qualified domain name and port to use to access the proxy or load balancer. The proxy or load balancer routes requests that it receives to QuickFile |
| Host name | If **Use a public facing domain name (FQDN)** is checked, type the proxy or load balancer host name or IP address where client traffic is routed. |
| Port number | Port to use to access the proxy or load balancer.<br>• If you configure a load balancer and SSL, set the port value to 9443. For a unsecure load balancer, define the port as 9080.<br>• If you configure Sterling Secure Proxy, set the port to the value defined in the Sterling Secure Proxy HTTP adapter. See “Protecting QuickFile with Sterling Secure Proxy” on page 32. |

## Configuring the timeout value for a session

You can change the timeout value. The timeout value identifies how long an inactive session remains valid.

### About this task

**Attention:** The System policy on the configuration section identifies how long an inactive session remains valid, in minutes. The default value is 30 minutes. The maximum value is 1440 minutes or 24 hours.

Use this procedure to set the timeout value.

### Procedure

1. Click **Configuration** from the menu.
2. Click the **System** tab.
3. Select a value in the **Length of time for user sessions before they expire** field. This value defines how many minutes before an idle session expires.
4. Click **Save**.
5. Restart QuickFile to enable the changes.

## Powering off or restarting QuickFile

You can restart or power off QuickFile.

### Before you begin

When possible, alert users in advance when you plan to restart or shut down QuickFile.

### About this task

For maintenance or other purposes, you might be required to restart QuickFile or power it off. Administration gives you the ability to accomplish this task in an orderly fashion. When possible, ensure that users are notified before you power down the server. Give users time to prepare for the temporary lack of access and to prevent file transfers from being affected.

To power off or restart the appliance, take the following steps:

### Procedure

1. Click **Configuration** from the menu.
2. Click the **Power** tab.
3. To restart QuickFile, click **Restart the appliance**.
4. To shut down QuickFile, click **Power off the appliance**. If you power off the appliance, you must restart QuickFile by using the VMware vSphere client.

## Use LDAP to manage users and passwords

Use QuickFile with your company lightweight directory access protocol (LDAP) server. It simplifies the tasks of adding and deleting users. Using LDAP user definitions better integrates the user experience of QuickFile into their workflow.

LDAP is an industry-standard Internet Protocol. It stores and accesses user information about a server. LDAP is widely used by email and other software programs for managing user address information.

If your company uses LDAP to manage users, you can use it to manageQuickFile users. With an LDAP connection, you can eliminate most of the requirement to add users or user groups to QuickFile.

If you enable LDAP, do not use QuickFile to manage LDAP users. Use the LDAP tools instead. If a user tries to log in to QuickFile with an expired LDAP password, the user is instructed to contact the administrator. As administrator, make sure that the user resets the password in the company (LDAP) directory.

**Restriction:** You can define users in both LDAP and through QuickFile. However, users that are created in LDAP cannot be managed in QuickFile and users that are created in QuickFile must be managed through QuickFile.

After you create a user in LDAP, request that the user login to QuickFile. The user profile is displayed when the user hovers over the picture and clicks **Profile**. Users can modify their profile, including name. This value is not required match the one defined in LDAP. Users cannot use the product to change their password. It is changed in LDAP.

## Configuring an LDAP server with QuickFile

As administrator, you can configure QuickFile to use your LDAP server. Using an LDAP server eliminates the requirement to add and maintain users in QuickFile. Users and password information are already created in LDAP; therefore, you do not have to create that information in QuickFile. You can define users in both LDAP and QuickFile.

### Before you begin

To use SSL with LDAP, enable SSL in the LDAP configuration. Then, import the LDAP server certificate into the truststore database in QuickFile from the **Configuration** menu, on the **SSL** tab. Also, set the LDAP server port to the SSL port used by the server.

### About this task

Complete the following steps to configure QuickFile to use your LDAP directory.

### Procedure

1. Click **Configuration** from the menu.
2. Click the **LDAP** tab.
3. To configure the LDAP connection, click **Connection Information** > **Enable LDAP integration**, and type information in the following fields.
   a. Server name
   b. Port number
   c. Principal ID
   d. Principal Password
4. To enable Secure Sockets Layer (SSL) for user authentication, check **Enable SSL**. Be sure to import the certificate into the truststore.
5. To test that your LDAP connection entries are valid, click **Test Connection**.
6. Click **Basic Information** and provide the following information:
   a. Type the **Group Base DN** to identify the group information that is specified in the LDAP database
   b. Type the **User Base DN** to identify the user information that is specified in the LDAP database
   c. To further identify a group within the base DN group, type the information in this text field and click **Enter**.
7. To add LDAP groups that you want QuickFile to recognize, click **Click to add**.
8. Click **Save**.

## LDAP configuration field definitions

The following definitions describe the fields on the **LDAP** tab of the QuickFile Configuration page.

| Field Name | Description |
|---|---|
| Enable LDAP integration | Check this box to allow the use the LDAP server. Clear the box to disable the option. Optional. The default is cleared. If you enable LDAP integration and configure it, LDAP users can use their LDAP credentials to sign in to QuickFile. |
| Server name | The host name or IP address of the LDAP server. It must be a valid LDAP server name in your network. (IPv6 is not supported.) Required. |
| Port number | Port number to use to access the LDAP server. Range of valid values is 1 - 65535. Required. |
| Principal ID | Fully qualified distinguished name of an LDAP user authorized to search the LDAP directory. Required. |
| Principal Password | Password for the principal ID. Required. |
| Enable SSL | Check to enable Secure Sockets Layer (SSL) security. If this option is enabled, you must import the LDAP server certificate into the QuickFile truststore. Optional. |
| Group Base DN | Group base distinguished name. The parent node where groups are stored in the **LDAP** field. Type the node as a fully qualified DN (ex: `OU=Users,O=IBM,C=US`). Required. |
| User Base DN | User base distinguished name. Enter the node as a fully qualified DN (ex: `OU=Users,O=IBM,C=US`). Required. |
| Group | Click **Click to add** and define the groups that are allowed to access QuickFile. Type the group as a fully qualified DN (ex: `CN=QuickFile Users, OU=Users,O=IBM,C=US`). Required. |
| Group Search filter class | Search filter for groups. Do not modify this value unless you are instructed to do so by Support. Default value: `(\|(objectClass=group)(objectClass=groupOfNames)(objectClass=groupOfUniqueNames))`.Required. |
| Member attributes | Array of attribute names. Do not modify this value unless support instructs you to do. |
| User Search filter class | Search filter for users. Do not modify this value unless you are instructed to do so by support. Required. Default value: `(\|(objectClass=user)(objectClass=person)(objectClass=inetOrgPerson)(objectClass=organizationalPerson))` |
| Email attributes | An array of email attribute names. Do not modify this value unless you are instructed to do so by support. |

# Setting up archiving

As administrator, you can set up QuickFile to archive all file transfer activity to ensure that a record of all activity is preserved.

### Before you begin

Setting up archiving requires FileNet. It also requires that you set up an appropriate FileNet document type for the archive. Finally, obtain the URL of the

CMIS service document that is used to access the archiving file system. Obtain the name of the archive top-level folder. For information, consult the FileNet documentation.

**Important:** Enabling archiving might significantly affect performance.

### About this task

To set up archiving, complete the following steps:

### Procedure

1. From the menu, click **Configuration**.
2. Click the **Archiving** tab.
3. Check **Enable an archiving system integration**. The fields for specifying archive information are activated
4. Select **FileNet**as the archive provider.
5. Type the **Service document URL** for the archive file system.
6. Type the name of the user who is authorized to access the archive system.
7. Type the user password for accessing the file system.
8. Type the **Top-level archiving folder** for the file system.
9. Click **Save**. Archiving is enabled. No system restart is required.

## Archiving field definitions

The following table describes the fields that you define to configure archiving on the Archiving tab of the Configuration features.

| Field Name | Description |
|---|---|
| Enable an archiving system integration | Check this option to enable archiving and activate the remaining fields on this page. |
| Archive provider | Select the database application to use to archive the files. Because FileNet is the only available provider, this field is display only. |
| Service document (URL) | The URL where the service document of the selected archiving system is located. Field is limited to 255 characters. |
| Repository ID | Repository identifier to which files and packages are archived. |
| Authorized username | User who is authorized to access the archive file system. Required. |
| Authorized password | The authorized user's password for accessing the archive file system. |
| Top-level archiving folder | Top-level folder where archived packages and files are stored. |

## FileNet integration

To integrate QuickFile with a FileNet repository, several custom properties and classes are required in the target FileNet repository.

FileNet must have the IBM CMIS for FileNet Content Manager bundled component installed. This component is available starting with FileNet Content Manager V5.0.

The following properties are required in the FileNet repository:

*Table 9. Custom properties*

| Property | Definition |
|---|---|
| `ibmmftPackageSender` | A single-value text property of a maximum 255 characters |
| `ibmmftSubject` | A single-value text property of a maximum 255 characters |
| `ibmmftSentOn` | A single-value date/time property |
| `ibmmftPackageRecipient` | A multiple value text property; each value can contain a maximum of 255 characters |
| `ibmmftMessage` | A single-value text property of a maximum 4000 characters |

The following classes are required in the FileNet repository:

*Table 10. Custom classes*

| Class | Definition |
|---|---|
| `IBMMFTArchiveDocument` | A subclass of the standard FileNet Document class. Must contain the five custom properties from Table 1. |
| `ibmmftPackageFolder` | A subclass of the standard FileNet Folder class. Must contain the five custom properties from Table 1. |
| `IBMMFTRootFolder` | A subclass of the standard FileNet Folder class. |

After the properties and classes are created in the FileNet repository, a top-level folder to hold the archived packages and files must be created. The top-level folder must be of type `IBMMFTRootFolder`. The name of the top-level folder is entered into the Archive configuration page in QuickFile.

## SSL configuration overview

QuickFile uses digital certificates to authenticate the identity of the server to a user that connects to it. SSL is a protocol for enabling secure communication sessions over an unprotected network, such as the Internet. To authenticate the server to users, obtain and check in digital certificates. Server certificates are stored in the keystore.

Certificates are used to secure communications and encrypt and decrypt data. Each certificate is made up of the public key and a private key. The public key contains the information that you send to your partner. The private key is saved at your site and confirms your identity. Always keep it secret.

As an added measure of security, obtain your certificate from a certificate authority (CA). A CA verifies all of the identity information in your certificate, then adds its signature. In an SSL transaction, your certificate is presented to each user who

connects to your server. The server recognizes the signature of the CA that signs the CA root certificate. Before you begin communicating with the user, make sure that the user site has a copy of the CA root certificate. The fact that the user recognizes your CA root certificate assures the user that you are who you say you are.

If you use a certificate that is not validated by a CA, it is called a self-signed certificate. Use self-signed certificates when identity verification is not required, such as communications within your company or during product testing.

To implement SSL when the transaction uses a CA certificate, import the CA root certificate into your truststore. If necessary, send the CA root certificate to the user, to include in the user truststore. Store your private key and CA certificate in the keystore. It is available for verification when you store it in the keystore.

## SSL configuration methods

Select the method to use to configure SSL. Methods include using a new CA certificate, an existing CA certificate, a chained certificate, or a self-signed certificate.

- If you have a CA-signed certificate that you used with another application, you can import it into QuickFile.
- If you do not have a CA-signed certificate, complete a signing request to request one. Extract the information from QuickFile and send it to the CA. After CA returns the signed certificate, import it into QuickFile. Enable SSL by identifying the server certificate and turn on SSL. All future connections authenticate the server to the incoming connection.
- To use a chained certificate, complete the chained certificate configuration. Enable SSL by identifying the server certificate and turn on SSL. All future connections authenticate the server to the incoming connection.
- For a less secure method, such as when you communicate with internal users or test an application, use a self-signed certificate for SSL authentication.

## Configure SSL by creating a new CA-signed certificate

To enable SSL authentication, use one of the following methods: request a new certificate from a certificate authority (CA) or use an existing CA-signed certificate to configure SSL authentication.

To request a new certificate from a CA and then configure SSL authentication in QuickFile:

- "Adding a certificate signing request"
- "Extracting a certificate from the signing request" on page 42
- "Selecting the certificate to use for server authentication" on page 43
- "Setting basic network configuration options" on page 29

### Adding a certificate signing request

To request a CA-signed certificate, complete a signing request. Then, send the request to the CA who signs it.

#### About this task

**Remember:** See the documentation of the certificate authority who signs your certificate signing request (CSR) to understand the CSR requirements. If the signing request does not meet the CA requirements, it might be rejected.

Complete the following steps to create a signing request and add it to the signed request store:

### Procedure

1. Click **Configuration** from the menu.
2. Click the **SSL tab**.
3. Click **Certificate Management** to expand the section.
4. Click the name of the signed request store to open.
5. Click **New**. The Certificate signing request page is displayed.
6. Type the key label to use when you reference this request in the **Key Label** field.
7. Type the common name that is used to reference the company or URL that is being validated in the **Common name** field.
8. Type information in the remaining optional fields as needed.
9. Click **Create**.

## New signing request field definitions

Create a signing request to create a certificate and send it to a CA to sign. The following table identifies the fields to define when you are creating a signing request.

| Field | Description |
|---|---|
| Key Label | Label to assign to the certificate signing request you create. |
| Key size | Key length that is required for the certificate public key to validate the key. |
| Common name | Fully qualified domain name (FQDN), host name, or URL to which you plan to apply your certificate. If the common name in the certificate does not match the value that is defined in this field, the session fails. |
| Organization | Name under which your business is legally registered. The listed organization must be the legal registrant of the domain name in the certificate request. If you enroll as an individual, type the certificate requester name in the **Organization** field. Type the DBA (doing business as) name in the **Organizational Unit** field. |
| Organizational unit | Define this field to differentiate between divisions within an organization. For example, "Engineering" or "Human Resources." If applicable, type the DBA (doing business as) name in this field. |
| Locality | Name of the city in which your organization is registered or located. Spell out the name of the city. Do not abbreviate. |
| State/Province | Name of the state or province where your organization is located. Type the full name. Do not abbreviate. |
| Postal Code | Postal code for the city in which your organization is located. |

| Field | Description |
| --- | --- |
| Country or region | Two-letter International Organization for Standardization (ISO) format country code for the country or region in which your organization is legally registered. |

## Extracting a certificate from the signing request

After you create a signing request, extract the certificate and send the information to the certificate authority (CA).

### About this task

Complete the following steps to extract the certificate from the signing request. You can then send it to the CA.

### Procedure

1. Click **Configuration** from the menu.
2. Click the **SSL** tab.
3. Click **Certificate Management** to expand the section.
4. Click the name of the signing request store where the CSR is stored.
5. Select the signing request to extract and click **Extract**.
6. Copy the text from the dialog and paste it into another file. Save the file.
7. Click **Close**.
8. Send the file to your CA and request that it is signed and returned to you.

## Uploading a keyfile received from a CA

Upload a keyfile received from a CA to make it available to QuickFile.

### About this task

To upload a key file from a CA:

### Procedure

1. Click **Configuration** from the menu.
2. Click the **SSL** tab.
3. Click **Certificate Management** to expand the section.
4. Click the name of the keystore to open.
5. Click **Upload key file**.
6. Enable **Import from a keyfile** and click **Browse** to locate the file.
7. Click **Upload**.

## Enabling or disabling SSL

After you configure your certificates and check them into the database, you then enable SSL. If you want to turn off SSL authentication, you can disable it.

### Procedure

1. Click **Configuration**.
2. Click the **SSL** tab.
3. If necessary, click **Configuration** to view the SSL configuration options.
4. Turn on **Enable secure connections (SSL)**.

5. To disable SSL, turn off **Enable secure connections (SSL)**.
6. Click **Save**. Restart your browser to activate the changes you made.

### Selecting the certificate to use for server authentication

You select the certificate that is used to authenticate the server. If certificates change, change the certificate setup.

#### Before you begin

To enable the certificate to use to authenticate the server to users who connect to the application:

#### Procedure

1. Click **Configuration** from the menu.
2. Click the **SSL** tab.
3. Select the certificate to use for authentication in the **Server certificate** field.
4. Click **Save**.

## Configure SSL by using an existing CA-signed certificate

To enable SSL authentication, use one of the following methods. You can request a new certificate, generate a chained certificate, or use an existing certificate to configure SSL authentication.

Complete the following procedures to use an existing CA-signed certificate to authenticate a connection and configure QuickFile to be authenticated by incoming connections:

- "Uploading a key file and importing a certificate"
- "Enabling or disabling SSL" on page 42
- "Selecting the certificate to use for server authentication"
- "Setting basic network configuration options" on page 29

### Uploading a key file and importing a certificate

To authenticate the QuickFile server with a certificate that you obtained from a CA, upload the CA key file into the database.

#### About this task

To upload a key file:

#### Procedure

1. Click **Configuration** from the menu.
2. Click the **SSL** tab.
3. Click **Certificate Management** to expand the section.
4. Click the name of the keystore where the certificate is imported.
5. Click **Upload key file**. The Upload key files dialog is displayed.
6. Enable **Import from a keyfile** and click **Browse** to locate the file.
7. Click **Upload**. The **Import Certificate** page is displayed.
8. Type information about the certificate, including key file name and password and imported certificate alias.
9. Click **Import**.

# Configure SSL with a chained certificate

To enable SSL authentication with a chained certificate, create a chained certificate and sign it with a root CA certificate. Then, you are ready to enable security with the chained certificate.

Complete the following procedures to create a new chained certificate and configure SSL authentication in QuickFile:

- "Configuring chained certificates"
- "Enabling or disabling SSL" on page 42
- "Selecting the certificate to use for server authentication" on page 43
- "Setting basic network configuration options" on page 29

## Use chained certificates

To increase security, you can use CA certificate chaining.

In certificate chaining, two or more CA certificates are linked in a certificate chain. The primary CA certificate is the root certificate at the end of the CA certificate chain. It must be present verify the authenticity of a certificate that is received. A certificate chain can be stored in a single file, such as a `.pem` file. It can be stored in separate files, where each file contains one CA certificate in the chain. If you intend to use certificate chaining, ensure that each CA certificate in the chain is installed in the truststore.

## Configuring chained certificates

To increase security, use a chained CA certificate. Before you create a chained certificate, import the key of the root certificate into the truststore. The root certificate is used to sign the chained certificate.

### About this task

To configure a chained certificate, complete the following steps:

### Procedure

1. Click **Configuration** on the menu.
2. Click the **SSL** tab.
3. Click **Certificate Management** to expand the section.
4. Click the name of the keystore to open.
5. Click **Create** > **Chained certificate**. The Create chained certificate page is displayed.
6. Type the alias that is used for this certificate in the **Alias** field.
7. Select the root certificate that is used to sign the certificate.
8. Type the common name to use for the chained certificate.
9. Select the key size of the root certificate from the list.
10. Type the common name to use for the chained certificate.
11. Type how many days the certificate is valid in the **Validity period** field.
12. If needed, type information about the server to validate in the remaining fields.
13. Click **Create**.

## Chained certificate field definitions

When you receive the certificate for another entity, you might be required to use a certificate chain to obtain the root CA certificate. The certificate chain is a list of certificates that are used to authenticate an entity. The chain begins with the certificate of that entity. Each certificate in the chain is signed by the entity that is identified by the next certificate in the chain. The chain ends with a root CA certificate. The root CA certificate is always signed by the CA itself. The signatures of all certificates in the chain must be verified until the root CA certificate is reached. The following table identifies the fields that you define when you configure a chained certificate in QuickFile.

| Field | Description |
|---|---|
| Alias | The alias that is associated with the certificate. The secure listener and connection definitions that specify SSL use the alias to reference the certificate. |
| Root certificate used to sign the certificate | The name of the root certificate. If the request does not include the complete certificate chain, the truststore is searched for the issuer certificates. |
| Key size | Size of the key that is used to sign the certificate. The following values are valid: 512, 1024, and 2048. Most certificate providers are moving to 2048-bit key sizes. |
| Common name | Fully qualified domain name (FQDN), host name, or URL to which you plan to apply your certificate. If the common name in the certificate does not match the value that is defined in this field, the session fails. |
| Validity period | How long the certificate can be used for authentication. Type the number of days, up to 365 days. |
| Organization | Name under which your business is legally registered. The listed organization must be the legal registrant of the domain name in the certificate request. If you enroll as an individual, type the certificate requester name in the **Organization** field. Type the DBA (doing business as) name in the **Organizational Unit** field. |
| Organization Unit | Define this field to differentiate between divisions within an organization. For example, "Engineering" or "Human Resources." If applicable, type the DBA (doing business as) name in this field. |
| Locality | Name of the city in which your organization is registered or located. Spell out the name of the city. Do not abbreviate. |
| State/Province | Name of the state or province where your organization is located. Type the full name. Do not abbreviate. |
| Postal Code | Postal code in which your organization is located. |

| Field | Description |
| --- | --- |
| Country or region | The two-letter International Organization for Standardization (ISO) format country code for the country or region in which your organization is legally registered. |

# Configure SSL by using a self-signed certificate

To enable SSL authentication by using a self-signed certificate, you create a self-signed certificate.

To create a self-signed certificate and configure SSL authentication in QuickFile:

- "Creating a self-signed certificate"
- "Enabling or disabling SSL" on page 42
- "Selecting the certificate to use for server authentication" on page 43
- "Setting basic network configuration options" on page 29

## Creating a self-signed certificate

For a quick way to test your environment, use a self-signed certificate. It is not signed by a CA and does not provide the security that is required in a production environment. If you use a self-signed certificate to test your environment, be sure to replace it before you use the product.

### About this task

To configure a self-signed certificate, complete the following steps:

### Procedure

1. Click **Configuration** from the menu.
2. Click the **SSL** tab.
3. Click **Certificate Management** to expand the section.
4. Click the name of the keystore to open.
5. Click **Create > Self-signed certificate**. The Create Self-signed Certificate page is displayed.
6. Type the alias to use for this certificate in the **Alias** field.
7. Select the common name that is identified in the certificate in the **Common name** field.
8. Type how many days the certificate is valid in the **Validity period** field.
9. If wanted, type information about the server in the remaining fields.
10. Click **Create**.

## Self-signed certificate field definitions

Create a self-signed certificate to enable SSL for an internal environment. A self-signed certificate is not as secure as using a CA certificate. However, it provides a level of security that can be used for testing and for validating the server to users inside the enterprise.

| Field | Description |
| --- | --- |
| Alias | The alias that is associated with the certificate. The secure listener and connection definitions that specify SSL use the alias to reference the certificate. |

| Field | Description |
|---|---|
| Version | Version that is used to create the self-signed certificate: `X509v3` or `IBMX509` |
| Key size | Key length that is required for the public key to validate the certificate. |
| Common name | Fully qualified domain name (FQDN), host name, or URL to which you plan to apply your certificate. If the common name in the certificate does not match the value that is defined in this field, the session fails. |
| Validity period | How long the certificate can be used for authentication. Type the number of days, up to 365 days. |
| Organization | Name under which your business is legally registered. The listed organization must be the legal registrant of the domain name in the certificate request. If you enroll as an individual, type the certificate requester name in the **Organization** field. Type the DBA (doing business as) name in the **Organizational Unit** field. |
| Organization Unit | Define this field to differentiate between divisions within an organization. For example, "Engineering" or "Human Resources." If applicable, type the DBA (doing business as) name in this field. |
| Locality | Name of the city in which your organization is registered or located. Spell out the name of the city. Do not abbreviate. |
| State/Province | Name of the state or province where your organization is located. Type the full name. Do not abbreviate. |
| Postal Code | Postal code for the city in which your organization is located. |
| Country or region | The two-letter International Organization for Standardization (ISO) format country code for the country or region in which your organization is legally registered. |

# Importing a certificate into the keystore

Specify a personal certificate to import from a keystore or key file. Upload the keyfile before you import a certificate.

## About this task

To import a certificate into the keystore:

## Procedure

1. Click **Configuration** from the menu.
2. Click the **SSL** tab.
3. Click **Certificate Management** to view the keystore and truststore.
4. Click **More** > **Import**. The **Import Certificate** page is displayed.

5. Type information in the following required fields:
   - Key file name
   - Key file password
   - Imported certificate alias
6. Click **Import**.

### Import Certificate field definitions

When you import a key file from a file, use the fields in the following table to import the certificate:

| Field | Description |
|---|---|
| Key file name | Name of the key file that contains the public key and the private key. |
| Type | Select the type of key to import: `JKS` or `PKCS12` |
| Key file password | The password that locks the key file and is used to import the certificate. |
| Get keyfile aliases | Click to query the key file for the aliases of all the personal certificates in the keystore. |
| Certificate alias to import | Certificate alias that is identified as the key file name that you want to import into the current keystore. |
| Imported certificate alias | New alias that you want the certificate to be named in the current keystore. |

## Signing the QuickFile Advanced File Transfer applet with your company code signing certificate

By default, the QuickFile Advanced File Transfer applet is signed by the code signing certificate that is provided by IBM. If preferred, you can replace the certificate with your company code signing certificate.

### About this task

Some company policies allow users to run only applets signed internally with their code signing certificate.

To override the default certificate with a certificate that you provide:

### Procedure

1. Upload a code signing certificate to the keystore, from **Configuration** > **SSL** > **Certificate Management**.
2. Import the code signing certificate to keystore, and name the certificate with an alias, for example, *onlycode*.
3. Create a properties file with the following entry:

   ```
   ssl.keyStore.codeSign.alias=onlycode
   ```

   Where *onlycode* is the alias you gave for the Code Signing certificate.
4. Upload the properties file to an SCP, FTP, or HTTP server that can be accessed from the QuickFile appliance.
5. On the VM console, run the startup wizard by entering `wizard startup.xml`

6. When prompted to configure the management network interface `eth0`, answer `n`.
7. When prompted to configure a DNS server, answer `n`.
8. When prompted to upload an IBM QuickFile configuration properties file, answer `y`.
9. Enter the protocol to use to upload the file to the appliance (`http, scp, or ftp`).
10. Enter the IP address or host name of the server where the properties file is located.
11. Enter the full path of the server where the properties file is located.
12. If the server where the properties file is requires authentication, answer `y`, otherwise answer `n`.
13. If the server requires authentication, enter the user name for authentication.
14. When prompted to download, review the information and answer `y` to proceed, or answer `n` if the information is incorrect and go back to the prompts.
15. For SCP, the first time that you transfer a file from the server, answer `yes` when prompted about trusting the server key.
16. If the server requires authentication, enter the password for the user.
17. When prompted about changing the admin password, answer `n`.
18. Restart the appliance by entering `device restart` on the console.

### Results

When the appliance restarts, the applet is signed with the specified code-signing certificate. If the certificate does not have the code-signing bit ON, the signing fails and the applet continues to be signed with the IBM provided certificate. After the applet is successfully signed with your code-signing certificate, the applet continues to be signed with that certificate with future firmware upgrades.

## Uploading a certificate file for storage

Upload a file into the keystore. The file is not available to use with application. It is only stored for future use.

### About this task

To upload a certificate file for storage, complete the following procedure:

### Procedure

1. Click **Configuration** from the menu.
2. Click the **SSL** tab.
3. Click **Certificate Management** to expand the section.
4. Click the name of the keystore where the file is uploaded.
5. Click **Upload key file**. The Upload key file page is displayed.
6. Enable **Just upload the file** and click **Browse** to locate the file.
7. Click **Upload**.

### Upload keyfile field definitions

Use the Upload keyfile window to define whether you are importing the uploaded files into the keystore or receiving the uploaded files from a CA.

| Field | Definition |
| --- | --- |
| Attach file to upload | To upload, do one of the following actions:<br>• Drag the keyfile to the **Attach** box<br>• **Browse** to select the keyfile |
| Select what you want to do with the file | Select the action to take with the file you are uploading:<br>• Receive from CA<br>• Import from a keyfile<br>• Upload the file |

## Deleting a certificate from the keystore

You can delete a certificate from the keystore to remove it.

### About this task

To delete a certificate from the keystore:

### Procedure

1. Click **Configuration** from the menu.
2. Click the **SSL** tab.
3. Click the name of the keystore that contains the certificate to delete.
4. Click the certificate to delete.
5. Click **More** > **Delete**. The Delete Certificate page is displayed.
6. Click **Delete**.

# Chapter 5. Use virus scanning to protect data

Virus scanning is the process of monitoring and preventing transfer of files containing viruses. You obtain services from a service provider and configure ICAP servers according to the service provider specifications. Use this server to implement policies for scanning files that are transferred by using QuickFile.

QuickFile can scan uploaded files for viruses. To scan files:

- Configure the ICAP server. The server can be configured for DLP scanning, antivirus scanning, or both.

  To configure the server, identify the following information:

  – Name to identify the server where the antivirus software is installed.
  – The provider who supplies the antivirus software.
  – The application that is installed on the server. Options include data loss prevention (DLP) or antivirus and DLP.

    **Restriction:** Duplicate ICAP servers cannot be configured. If a server is configured for antivirus and DLP, you cannot add a single antivirus or single DLP configuration.
  – Information about the server includes the host name, service name, and port number.

  See Chapter 7, "Activating a virus scan or data loss prevention server," on page 55 for instructions on configuring the ICAP server.
- Test the server configuration to determine whether the definition connects to the ICAP server.
- Before you configure a policy, activate the server.
- To configure a sample policy without enabling it, do not activate the server.
- Configure a policy to define which files to scan. You can scan all uploaded files or scan only uploaded files from internal users.

  **Restriction:** If the server is not configured, you cannot define a policy.
  See "Policy for antivirus scans" on page 62 for instructions on setting the policy.
- After you configure a server and define a policy, files are scanned according to the policy you defined. You can set the policy to scan all incoming files or only incoming files from external users. If the scan identifies that there is a virus in a file, the following actions occur:

  – The file transfer is canceled.
  – A status of **Package failed** is displayed on the Sent files page next to the transfer that is canceled.
  – The file logs identify any transfers that are canceled because of a failed virus scan.

# Chapter 6. Use DLP scanning to prevent data loss

Data loss prevention (DLP) is the process of monitoring and preventing sensitive data from leaving your company server. You obtain services from a service provider and configure ICAP servers according to the service provider specifications. Use this server to implement policies for scanning files that are transferred by using QuickFile.

QuickFile can scan uploaded files for DLP. To scan files:

- Configure the ICAP server. The server can be configured for DLP scanning, antivirus scanning, or both.

  To configure the server, identify the following information:

  – Name to identify the server where the DLP software is installed.
  – The provider who supplies the DLP software.
  – The application that is installed on the server. Options include data loss prevention (DLP) or antivirus and DLP.

    **Restriction:** Duplicate ICAP servers cannot be configured. If a server is configured for antivirus and DLP, you cannot add a single antivirus or single DLP configuration.
  – Information about the server includes the host name, service name, and port number.

  See Chapter 7, "Activating a virus scan or data loss prevention server," on page 55 for instructions on configuring the ICAP server.
- Test the server configuration to determine whether the definition connects to the ICAP server.
- Before you configure a policy, activate the server.
- To configure a sample policy without enabling it, do not activate the server.
- Configure a policy to define which files to scan. You can scan all uploaded files or scan only uploaded files from internal users.

  **Restriction:** If the server is not configured, you cannot define a policy.
  See "Policy for data loss prevention (DLP) scans" on page 63 for instructions on setting the policy.
- After you configure a server and define a policy, files are scanned according to the policy you defined (all files or only files from internal users). If the scan identifies that there is sensitive company data in a file, the following actions occur:

  – The file transfer is canceled.
  – A status of **Package failed** is displayed on the Sent files page next to the transfer that is canceled.
  – The file logs identify any transfers that are canceled because of a failed DLP scan.

# Chapter 7. Activating a virus scan or data loss prevention server

Configure the ICAP servers to use for virus scanning or data loss prevention.

## Before you begin

The Internet Content Adaptation Protocol (ICAP) is a lightweight HTTP-based protocol that implements virus scanning and data loss prevention. The following prerequisites apply:

- Obtain services from a supported ICAP provider.
- Determine the configuration setting your services provider requires for the services.
- Configure QuickFile to match your provider setup for the ICAP servers that are used for virus scanning and data loss prevention (DLP). You can configure one ICAP server to process both services or one server for each service you implement, depending on your service provider. For example, certain providers configure antivirus and DLP on the same server. For these providers, you configure only one ICAP server.

When you configure the server, identify which services are provided:

- Antivirus scanning
- DLP
- Both antivirus scanning and DLP

## About this task

To configure the services that are required for your environment:

## Procedure

1. Click **Configuration** from the navigation menu.
2. Click the **ICAP Servers** tab.
3. Click the **Add ICAP server** button to open the page and define a new server.
4. To enable the use of the configured server, confirm that the **Activate ICAP server** box is selected.
5. Complete the fields according to the definitions. See "ICAP server configuration fields" on page 56 for more information.
6. To test whether the QuickFile server can connect to the ICAP server, click **Test Configuration**.
7. Click **Save**.

## What to do next

Set a policy that uses the server you configure. See:

- "Policy for antivirus scans" on page 62
- "Policy for data loss prevention (DLP) scans" on page 63

## ICAP server configuration fields

When you configure or edit an ICAP server definition, complete the following fields:

| Field | Description |
|---|---|
| **Server name** | Name that is assigned to the ICAP server. Any value update to 100 characters. Required. |
| **Provider name** | Name of the provider of the virus scan or DLP software. Select a provider from the list:<br>• Symantec Data Loss Prevention<br>• McAfee Web Gateway<br>• Symantec Protection Engine<br>Required. |
| **Server type** | The services that are provided by the server you configure. Select a type from the list:<br>• Antivirus<br>• Data Loss Prevention (DLP)<br>• Antivirus and DLP<br>Required.<br>**Tip:** Only the choices that are valid with your selected provider are available. |
| **Host name (IP Address)** | Host name or IP address that is used to connect to the ICAP server. The value that is allowed for a host name is up to 255 characters. Each dot-separated segment can be no longer than 63 characters. The last segment must be longer than two characters.<br>For an IP address, the value can be up to 15 characters, must include 4 dot-separated segments that consist of only numbers. Each segment includes a value from 0 to 255.<br>Example values include the following values: `myhost`, `myhost.company`. `domain.com`, or 192.168.1.1.Required. |

| Field | Description |
| --- | --- |
| **Service name** | Name of the ICAP service to use at the server you configure.<br><br>It also is used in the ICAP URL path.<br><br>For example: `icap://server:port/serviceName` is the URL value. This field includes up to 255 characters. The value must begin with an alphanumeric character. The following characters are allowed:<br>• Alphanumeric<br>• / (slash)<br>• _ (underscore)<br>• - (hyphen)<br><br>A few examples are the following values:<br>• McAfee Web Gateway - `RESPMOD`<br>• Symantec antivirus - `SYMCSCANRESPEX-AV`<br>• Symantec DLP - `reqmod`<br><br>**Tip:** The values for **Service name** are set by your service provider.Required. |
| **Port number** | The port where the ICAP server is configured to accept connections. Allowed values are an integer number 1025 - 65536. The default value is 1344. Required. |
| **Scan chunk size** | How to break up the file for transmission to or from the server. Must be an even multiple of 1024, with a maximum of 1048576 (1024 X 1024). The default value is 8192. Required. |
| **Test Configuration** | Click **Test Configuration** to test whether the QuickFile server can connect to the ICAP server. |

# Chapter 8. Policies that define settings for all users

Define global user policies to identify how users interface with QuickFile at your installation.

As administrator, you can define policies to set system-wide user settings and define how QuickFile works for all users. You can also define groups and apply policies to a set of users with the same requirements.

**Restriction:** Not all policies can be applied to a group of users.

You can configure the following policies:

- How to set external user account expirations
- How to manage users who enter incorrect login information and are locked out of the system
- Password reset options
- The password strength that is required and how long a password is valid
- Run, edit, suspend, and resume common administrative schedules, such as when to clear the database and delete expired transfers
- The type of users that can invite external users to register
- The type of users that is authorized to send files to internal and external users
- The largest size file that can be uploaded

## Policy for external account expiration

Define an account expiration policy to identify if external user accounts expire. If an account expiration policy is defined, all external users expire after the amount of time you defined in the length field.

As administrator, you can define a policy to determine whether external user accounts expire and how long accounts are active. Consider the following information when you configure a user account policy:

- A mail domain must be defined in the advanced network options to before you can configure this policy.
- If no account expiration policy is defined, external user accounts do not expire.
- If an expiration policy is defined, an external user account is valid from the time the account is created until the expiration period elapses.
- The first expiration policy that is defined is applied to all existing external user accounts.
- This policy applies to all external users who are sent a file, invited to send a file, and requested a file.
- Users are notified seven days before the account is expiring.
- If the account expire period is less than seven days, the expiration email is sent out immediately.
- You can change the expiration date for all user accounts. For example, if the accounts expire in 30 days and 20 days elapses, you can change the expiration time to 60 days. The account then expires in 60 days.
- When an external account expires, the user can no longer log in to QuickFile

- Internal users do not expire.
- When an external user account expires, all users who received files from the expired user have access to the received files until the file expires.
- After an external user account expires, the account is no longer available. However, the external user can register with the same credentials and begin to send and receive files again. The newly activated external user cannot access files that are sent before the account expires.
- Administrative accounts are exempt from this policy and do not expire.

Ensure that you define an internal mail domain server. Otherwise, you cannot define an account management policy

## Creating a user account expiration policy

Use the account expiration policy to define whether external user accounts expire. First, enable the option. Then, define the expiration length. Use this policy to define how long a user account is active before it expires.

### About this task

**Remember:** Define at least one mail domain server before you create an account expiration policy. Use the network configuration to set the mail domain server. See "Configuring advanced network options to define internal users" on page 30.

To configure the user account expiration policy:

### Procedure

1. From the navigation menu, click **Policies**.
2. Click the **Account Management** tab.
3. Expand the Account Expirations section.
4. Enable the **Enable expiration of external user accounts** field.
5. In the **Length of time before external user accounts expire** field, select an expiration value from 1 - 999 and select the unit. The default value is 30 days.
6. Click **Save**.

## Disabling an expiration policy of external user accounts

After you define an account expirations policy, you can disable it if you no longer want external user accounts to expire. If an account was configured to expire, disabling the policy prevents all external user accounts from expiring.

### About this task

To disable the user account expiration policy:

### Procedure

1. From the navigation menu, click **Policies**.
2. Click the **Account Management** tab.
3. Expand the Account Expirations section.
4. Clear **Enable expiration of external user accounts**.
5. Click **Save**.

## Account expiration field definitions

The account expiration fields on the **Account Management** tab describe the information that is defined to configure the expiration length of external user accounts.

| Field Name | Description |
|---|---|
| Enable expiration of external user accounts | Select this option to turn on the expiration of an external user account. |
| Length of time before external user accounts expire | In the first box, define the length of time that an external account remains active. Valid values are 1 - 999.<br><br>In the second box, define the unit of measure as days, months, or years.<br><br>If this definition is the first policy definition, it is immediately applied to all external user accounts. The user account policy is applied to each newly created external user account. |

# Policy for account lockout

As administrator, you can set a policy to define whether users are temporarily blocked from logging in. The policy is enforced after the user fails to log in correctly a defined number of times.

You set how many failed logs in attempts a user can try before the user is locked out. You can define how long the user is locked out.

## Setting user lockout policies

Set a temporary user account lockout policy to define when a user is locked out. The lockout occurs after a user attempts to log in multiple times with invalid credentials.

### About this task

For security reasons, you can temporarily lock a user out of QuickFile. The lockout occurs if the user fails to provide a valid user ID and password. You define how many tries the user is allowed to provide invalid credentials before the user is locked out. This practice discourages malicious parties from guessing at possible passwords to access an account.

To set the lockout policy:

### Procedure

1. Click **Policies**.
2. Click the **Account Management** tab.
3. Expand the **Temporary Lockouts** section.
4. Select **Password lockouts** to enable lockout.
5. Define values in the following fields:
   - **Number of failed login attempts before lockout**
   - **Duration of temporary lockout**
   - **Time before failed login attempt counter resets**
6. Click **Save**.

## Temporary lockouts field definitions

To define when a user is locked out of QuickFile after incorrectly entering login information, configure the Account Management page, **Temporary Lockouts** section.

| Field Name | Description |
|---|---|
| Password lockouts | Enable or disable password lockout. Optional. |
| Number of failed login attempts before lockout | How many times the user can unsuccessfully try to log in before the user is locked out. If **Password lockouts** is enabled, select a number 1 - 99 in this field. |
| Duration of temporary lockout | The time that must elapse before the user is allowed to attempt to log in again after the user is locked out. Select a value 1 - 99 and units as minutes or hours for the duration. |
| Time before failed login attempt counter resets | The time during which failed login attempts are counted, starting with the first failed attempt. The failed attempt counter resets to zero when this time elapses. Select a value 1 - 99 and units as minutes or hours for the time period. |

# Policy for antivirus scans

After you configure antivirus software, define which files to scan for viruses. After files are scanned, any transfer that has an infected file is canceled.

### Before you begin

First, define the ICAP server. The information that is required to configure the policy might change based on the options you define in the ICAP server setup. You can create a policy when the server and provider are configured but the provider is not activated. However, virus scanning is not activated until the provider is activated. See Chapter 7, “Activating a virus scan or data loss prevention server,” on page 55 for instructions on enabling the ICAP server.

- If a provider and servers are defined but the provider is not active, you can define the policy but no scans occur. Scan begin after the providers are activated.
- If a provider is not defined, or a provider is defined but no servers are set up, the policy settings are not displayed. You cannot define a policy.

### About this task

To define the files to scan for viruses, complete the following steps:

### Procedure

1. Click **Policies** from the navigation menu.
2. Click the **File Security** tab.
3. Under **Antivirus**, check the **Enable antivirus scanning for file transfers** option, if you want to immediately implement this policy.
4. Enable one of the following options to define which files are scanned for viruses:
   - **Scan all incoming files** to scan all incoming files for viruses

- **Only scan incoming files from external users** to scan only files that are received from external users

5. Click **Save**.

## Policy for data loss prevention (DLP) scans

After you configure the data loss prevention (DLP) server, define which files to scan for data integrity. When files are scanned, any transfer that includes sensitive information is canceled. Only uploaded files can be scanned.

### Before you begin

Configure the ICAP server before you define a policy. The provider must be activated before you can define the policy. See Chapter 7, "Activating a virus scan or data loss prevention server," on page 55 for instructions on enabling the ICAP server.

### About this task

To define which files to scan for DLP:

### Procedure

1. Click **Policies** from the navigation menu.
2. Click the **File Security** tab.
3. Expand the **DLP** section.
4. In the **DLP** subsection, check the **Enable DLP scanning for file transfers** option, to immediately activate this policy.
5. Select a scan policy for file transfers:
   - **Scan all uploaded files** to scan all files for data loss prevention.
   - **Only scan uploaded files from internal users** to scan all files uploaded from all internal users.

   **Restriction:** There is no option for scanning for files coming in from an external source.
6. Click **Save**.

## Policy for maintenance task schedules

As administrator, you can schedule predefined tasks to run regularly. These tasks keep QuickFile running efficiently to meet business requirements.

### About this task

Configure QuickFile to use predefined maintenance tasks on a regular schedule. The list of tasks is defined by QuickFile. You configure the maintenance tasks to schedule for your environment. You can start a task manually, set up a schedule by which to run a task, and suspend and resume tasks. The default state for all tasks is Scheduled.

### Procedure

1. Click **Policies** from the navigation menu.
2. Click the **Schedules** tab.

3. Select **Show all tasks**. QuickFile provides the following methods to set up schedules:

*Table 11. Scheduling methods for maintenance tasks*

| Scheduling Method | Description |
|---|---|
| Predefined | Use predefined intervals as a simple method to define a schedule. Select one of the following predefined intervals:<br>• Yearly to schedule a task one time per year at 12:00 a.m. on 1 January<br>• Monthly to run a task on the first day of every month at 12 a.m.<br>• Weekly to run a task every Sunday at 12:00 a.m.<br>• Daily to schedule the task at 12:00 a.m. every day<br>• Hourly to schedule the task at the beginning of every hour |
| Interval | Options that allow finer control over scheduling. You can run a task every x minutes or hours, and every day or every weekday. |
| Date-Time | Identifies specific days of the week when the task is run. You choose the days of the week and the times to run the task. For example, set a task to run each Tuesday and Thursday at 6:00 a.m. and 6:00 p.m. |
| CRON | A notation method that uses a limited set of characters in a special syntax to express scheduling times.<br><br>This application supports CRON notation to define date and time intervals and specifies six terms to define the expression. While other approaches to CRON use five terms, this application requires six terms and does not support five terms. Consult the WebSphere Application Server documentation and search on the topic title: Interface User Calendar.<br><br>**Important:** Because of the complexity of CRON expressions, QuickFile uses only limited validation of your entries. |

4. Click **Save**.

## Tasks available to schedule

Set policies for QuickFile to complete predefined system-wide maintenance tasks on a regular schedule. The list of tasks is defined by QuickFile.

The default state for all tasks is **Scheduled**, with a default interval.

A drop-down menu next to the **Status** provides the following choices:

- Run - to start a task manually
- Edit - to change the schedule

- Suspend - to stop a task that is running and resume it later
- Resume - If you suspend a task, you must manually resume it.

The following table describes the tasks that are scheduled to run. Change the value of each task to prevent the task from running.

| Task | Description |
|---|---|
| **Lifecycle** | An update to the status of file transfers through the following states:<br>• Processing<br>• Number of files that are sent or received (indicates a successfully completed transfer)<br>• Transfer Failed (indicates that a virus scan or data loss prevention scan found a problem in a file in a package)<br>The default interval is every 30 seconds. |
| **Notification** | Queues all outstanding email notifications and prepares them to be sent. The default interval is every 30 seconds. |
| **Purge** | Marks all packages that expired and any incomplete file transfer packages and makes them available for deletion. An incomplete package is one that was sent but was interrupted and did not complete the transfer within seven days. It cannot be downloaded. All packages marked for deletion are removed from the database. The default interval is hourly. |
| **PurgeEvents** | Removes system events from the logs according to the configuration of **System Events Purge**. A comma-separated file with a list of the events that are purged is sent to all system administrators. An email notification that the **PurgeEvents** task completed is sent to all system administrators. The default interval is daily. See “Configuring event purge” on page 67. |
| **Reminder** | Queues all outstanding reminder email messages and makes them available to send. The default interval is every 30 minutes. |
| **Status** | Batch removal of database records after they are no longer required. The default interval is every 5 minutes. |
| **User** | Performs maintenance of user and group-related records. The types of record maintenance include the following examples:<br>• Removing user registrations that are expiring<br>• Identifying expiring SSL certificates<br>The default interval is every day at 4 AM. |

## Scheduling maintenance tasks

Use the **Schedule** tab under **Policies** to set schedules to fit your requirements for the tasks QuickFile must complete regularly.

### About this task

QuickFile must routinely perform certain tasks, in order for the system to function smoothly and maintain performance. Maintenance tasks are scheduled to run on a default schedule. The task scheduler can set up a custom schedule for each task. You can also suspend or resume a task, or set it to run immediately.

To define scheduling or to manually run a task:

### Procedure

1. Click **Policies** on the menu.
2. Click the **Schedules** tab.
3. By default, only scheduled tasks are displayed in the schedule list. Click **Show all tasks** to view the full set of tasks.
4. To immediately run a task, select the task and click **Run**.
5. To define a custom schedule to use for a task in the list, complete the following steps:
   a. Enable the task and click **Edit**.
   b. Click the tab of the scheduling method to use.
   c. Set up the interval to use to run the task. See "Policy for maintenance task schedules" on page 63 for information about the scheduling methods and options.
   d. Click **Save** to save your changes.

      **Tip:** You are not required to restart QuickFile for the changes to take effect.

### What to do next

If you detect that scheduled tasks are not running or are running at unpredictable intervals, and the hypervisor is ESXi5, take the following actions:

- Ensure that the hypervisor NTP server is configured and running.
- Verify that the QuickFile NTP server and underlying hypervisor are using the same NTP server.

## Suspending or resuming a task

You can suspend a task that is running or restart a task that is suspended.

### About this task

QuickFile must routinely complete certain tasks, in order for the system to function smoothly. After you schedule tasks to run regularly, you can suspend a task and resume it later.

To suspend a task and restart it later, complete the following procedure:

### Procedure

1. Click **Policies** on the menu.
2. Click the **Schedules** tab.

3. Enable the task to suspend and click **Suspend**.
4. To restart the task, complete the following steps:
   a. Click **Show all tasks** to view all tasks.
   b. Enable the task to restart and click **Resume**.

## Configuring event purge

System events can be purged and exported to reduce the number of events that are listed in logs and maintain performance of your system.

### About this task

Event purging is enabled by default. To resume **PurgeEvents** if the schedule is suspended, or to change the length of time events are retained:

### Procedure

1. From the **Administration** menu, select **Policies** and click the **Schedules** tab.
2. Click **Show all tasks**.
3. To confirm purging of system events, verify **Resume** is selected for **PurgeEvents**. The label states **Scheduled**.
4. When **PurgeEvents** is set to **Scheduled**, from the **Administration** menu, select **Configuration** and click the **System** tab.
5. To change the event retention time, select from the following values, in number of days:
   - 15
   - 30 (default)
   - 60
   - 90

   The **PurgeEvents** task purges events based on the interval you set. The task purges events that are in the system for a number of days that exceeds your setting for retention time. The default is for the task to run weekly on Sundays at midnight to purge events older than 30 days. See "Scheduling maintenance tasks" on page 66.
6. Click **Save**.

   **Tip:** The changes take effect immediately, without a restart.
7. You can set the **PurgeEvents** task to run one time immediately by selecting **Run**.

### Results

An email notification is sent to all system administrators when **PurgeEvents** completes, if the following conditions are met:

- The administrator email account is valid and configured
- Email notifications are enabled in the administrator user profile

The email notification includes a link to download a CSV file containing exported events. Exported log files are also available for download from the Received files list for all administrators. The exported log files have the following characteristics:

- A maximum file size (100 MB). If the purged events list exceeds the maximum file size, multiple files are generated. Each file is listed separately in the Received files list and generates a separate email notification.

**Restriction:** The maximum file size for the purged events list is not governed by the system maximum file size setting.

- CSV format
- An expiration time of 90 days.

  **Restriction:** After 90 days, the files are unrecoverable except from archives (if archiving is enabled).
- The file name is `archived-events-`*`timestamp`*`.csv`, where *timestamp* is in the format `yyyyMMdd_HHmmss`

**Important:** When you upgrade from a previous release, events from the previous release are moved to the new installation. The same settings for **PurgeEvents** apply to these events. Depending on the age of events in your system, the first run of the **PurgeEvents** task purges the events that are moved.

## Task scheduler field definitions

Define the fields on the Schedules tab of Administration Policies to define what tasks are displayed and how often to run the schedule.

| Field Name | Definition |
|---|---|
| Show only scheduled tasks | Click this option to show only tasks with an established schedule. Default. |
| Show all tasks | Click this option to show all tasks regardless of whether their schedule is defined. Optional. |
| Name | The name of the task. The tasks in this list are determined by the server and are not editable. Tasks cannot be added or removed. Click the task name to edit its schedule. The following values are valid:<br>• **Lifecycle**<br>• **Notification**<br>• **Purge**<br>• **PurgeEvents**<br>• **Reminder**<br>• **Status**<br>• **User** |
| Status | Indicates whether a schedule is set up for the task and whether the task is running or suspended. The following values are valid:<br>• **Scheduled**<br>• **Not Scheduled**<br>• **Running**<br>• **Suspended** |
| Interval | The schedule interval. See "Policy for maintenance task schedules" on page 63 for possible values for this field. Display only. |
| Next run | The date and time when the task is next scheduled to run. Expressed as a date (or Today if so scheduled) and a time. Display only. |

# Policy for password requirements

As administrator, you can set a policy to define the requirements for a valid password.

You can include one or more of the following password requirements:

- Password strength
- Password complexity definition
- Minimum and maximum duration
- How many passwords in history cannot be used in the password reset
- If a user is allowed to reset a password and how long

## Setting a password policy

As administrator, you can define the policies that are used to define the passwords.

### About this task

QuickFile provides the method to set policies on secure user access. Password policy settings manage requirements for password strength and duration and set parameters to use to reset passwords.

If your environment uses the lightweight directory access protocol (LDAP) to manage users and passwords, use LDAP to configure QuickFile users. Users who log in using LDAP credentials are managed by LDAP and not by QuickFile policies. Therefore, LDAP users must use LDAP to reset their password. If an LDAP user logs in with an expired password, the user is notified by QuickFile and instructed to contact the LDAP Administrator.

Complete the following procedure to set password policies:

### Procedure

1. Click **Policies** on the menu.
2. Click the **Password** tab.
3. To set password strength requirements:
   a. Click **Strength** to display strength options.
   b. Type a value in **Minimum characters in passwords** field.
   c. Define the types of characters users must include in a valid password in the characters options.
   d. If required, type a value in the **Maximum same character allowed consecutively** and **Maximum occurrences of the same character** to define a consecutive character limit and total character limits.
4. Complete the following steps to set how long a password is valid:
   a. Click **Duration**.
   b. Set the minimum change limits, minimum time between password changes, and how many passwords to keep in history.
   c. Set the maximum duration requirements in the password expirations, password expires in. Set the password expiration warning.
5. To set password reset requirements, click **Reset** and set one or more of the following reset requirements:
   a. To allow users to reset their password, enable **Allow users to reset passwords**.

b. To prevent users from resetting their password, disable **Allow users to reset passwords**.
c. To set **Time before password reset request expires**, select how many and the units of time.

6. Click **Save**.

## Password policy field definitions

Use the following definitions on the **Password** page. Type a zero in a field if you do not want to require that definition in the password.

| Field Name | Description |
|---|---|
| Minimum characters in passwords | Minimum number of characters a password must contain. Range is 6 - 128.<br><br>The total of lowercase, uppercase, numeric, and special characters that are specified in the following four fields cannot exceed this value.<br><br>Required. |
| Minimum lowercase characters | Minimum number of lowercase characters the password must contain. Range is 0 - 128.<br><br>Optional. |
| Minimum uppercase characters | Minimum number of uppercase characters the password must contain. Range is 0 - 128.<br><br>Optional. |
| Minimum numeric characters | Minimum number of numeric characters the password must contain. Range is 0 - 128.<br><br>Optional. |
| Minimum special characters | The minimum number of special characters the password must contain. Range is 0 - 128.<br><br>The following are considered special characters: ~ `! @ # $ % ^ & * ( ) - _ + = { } [ ] \| \: ; " ' < >,. ? /<br><br>Optional. |
| Maximum same character allowed consecutively | Maximum number of consecutive instances of the same character that is allowed in the password. Range is 0 - 128.<br><br>Zero indicates no limit on consecutive characters.<br><br>Optional. |
| Maximum occurrences of the same character | The maximum number of any character that the password can contain. Range is 0 - 128.<br><br>Zero indicates no limit on repetitions of a character. Optional. |

| Field Name | Description |
| --- | --- |
| Enable minimum change limits | Check this box to set a minimum time between changes of the user password and to enable the password history.<br><br>Optional. |
| Minimum time between password changes | Minimum time that must elapse between changes of a user password. Select the number (1 - 100) and units (minutes, hours, days, weeks, months, years).<br><br>If **Password expirations** is checked, the value that is specified here cannot exceed the value in **Password expires in**.<br><br>If **Password expirations** is not checked, the value that is specified here cannot exceed 30 days. Optional. |
| Number of passwords kept in history | How many former passwords are kept in history. Range is 0 - 99. Optional. |
| Enable password expirations | Check this box to set a maximum time between changes of the user password. Optional |
| Password expires in | Time within which users must change their password. Select a number 1-365 and units in hours, days, weeks, months, or years. |
| Warn users before password expires | Generate a warning in advance of the expiration of a user password (based on the setting in Password expires in). Select 1-30 days. |
| Allow users to reset passwords | Check this box to allow users to reset their password. Optional. |
| Time before password reset request expires | Time after which a user request to reset a password expires. When a user clicks **Forget your password?** on the Login page, QuickFile sends the user an access code. The user must click the link in the email and change the password within this time and provide the access code to reset the password. Select a number (1-100) and units (minutes, hours). Optional. |

## Policies for file transfer expiration and file size

As an administrator, you can set system-wide policies that affect when file transfers expire. You can also define whether notifications are sent to users when their files are about to expire. You can set whether users can choose to be notified when they receive files. You can also set a maximum size for individual files that users are allowed to send.

### About this task

To set system management policies, complete the following procedure:

### Procedure

1. Select **Policies** from the menu.
2. Click the **System Management** tab.
3. To manage file expirations:
   a. Click **Expirations** to expand the section.
   b. Set the default file expiration period by selecting the number and units for **Default expiration for all files sent by system users is**.
   c. To allow users to override the default expiration, enable **Allow end users to override the default file expiration length**.
4. Complete the following steps to define when expiration notifications are sent:
   a. Click **Expiration Notifications** to expand the section.
   b. Set a final notification by enabling **Send final warning notification before the transfer expires**. Select how long before a file transfer expires the final notification is sent.
   c. Set an initial notification by enabling **Send initial warning notification before the transfer expires**. Select how much time before expiration the initial notification is sent.
   d. To change the frequency of notifications, click the arrows to set the number of units, and select the units from the following values:
      - Hour
      - Day
      - Week
      - Month
      - Year

      See "Policy for maintenance task schedules" on page 63.
5. To set that maximum file size that can be transferred, click **File Size** and type a maximum size in megabytes.

   **Note:** Not all browsers support this feature. For browsers that support a limit on the size of file transfers, refer to System requirements
6. Click **Save**.

## Policies for user management

Manage user policies including who can send files to an unregistered user, if an unregistered user can receive files, and who can invite an unregistered user to register.

Use the following procedures to manage user policies:

- "Defining file transfer restrictions"
- "Defining users who are allowed to send registration invitations" on page 73

### Defining file transfer restrictions

Define the type of users who can send a file transfer and what type of user can receive the files.

### About this task

Use this procedure to define who can transfer files and request files from unregistered users. You can prevent external users from receiving files. The default value is allowing everyone to send and receive files. You can prevent external users from sending files or receiving files.

Complete the following procedure to define file transfer restrictions:

### Procedure

1. Click **Policies** from the menu.
2. Click the **User Management** tab.
3. Click **File Transfers**.
4. To define who is allowed to send files to external users, select one of the following options:
   - To prevent external users from sending files to other users, select **Only internal users can send files to external users**.
   - To allow any registered user to send files to anyone, select **Internal and external users can send files to anyone**.
5. To define who is allowed to receive files transfers, enable one of the following options:
   - To prevent unregistered users from receiving files, enable **File transfers cannot be sent to unregistered users**.
   - To allow all users to send file transfers, enable **File transfers can be sent to anyone**.
6. Click **Save**.

## Defining users who are allowed to send registration invitations

Define which users can send registration invitations by defining them in the User Management policy. A user who registers is allowed to send and receive files, if the administrator activates permissions. A registered user can also view information about how many file transfers were sent and received.

### About this task

The User Management policy identifies:

- Which users can send registration invitations
- Whether internal users can send files to external users
- Whether file transfers can be requested or sent from unregistered users
- How long an unregistered user is allowed to register after the user receives an invitation

To set the User Management policy:

### Procedure

1. Click **Policies** from the menu.
2. Click the **User Management** tab.
3. Click **Invitation to Register**.
4. Enable one of the following options

- To prevent users from sending registration invitations, enable **Disallow users to invite others to register**.
- To allow only internal users to send registration invitations, enable **Only internal users can invite others to register**.

  **Restriction:** If the internal domain is not specified, all users except admin users are considered external. If you select this option, only admin users can send invitations.
- To allow all users to send registration invitations, enable **Allow users to invite others to register**.

5. Define how many days an invitation is active in the **Invitations to register expire in** field.
6. Click **Save**.

## File transfer policy field definitions

The File transfers settings on the **User Management Policies** page define who can send file transfers to external users.

| Field Name | Description |
|---|---|
| Only internal users can send files to external users | Select this option to allow only internal users the ability to send files to users outside of the company. |
| Internal and external users can send files to anyone | Select this option to allow both internal and external users to send files to one another. An internal user is defined on the domain within the company. An external user is a user outside of the company server. |
| File transfers cannot be sent to unregistered users | Select this option to prevent file transfers from being sent to unregistered users. |
| File transfers can be sent to anyone | Select this option to allow all users to send files to unregistered users. |

## Invitation to register policy field definitions

You can configure fields in the invitation to register policy to define who can invite an external user to register.

| Field Name | Description |
|---|---|
| Disallow users to invite others to register | Prevents all users from requesting that another user register. |
| Only internal users can invite others to register | Allows only internal users the ability to send a request to register to an external user. |
| Internal and external users can invite others to register | Allows all users to invite other users to register. |
| Invitations to register expire in | Identify when an invitation expires. Default is 7 days. Enter the number of units and select the unit of measure: hours, days, weeks, months, years. |

# Chapter 9. Manage user accounts

As administrator, use the Users page to add users and permanently lock users from the system. You can also reset a user registration, assign administrative rights, set authentication type, and delete a user.

You can add individual users to QuickFile. Define whether the user is an administrator or regular user. You can also define whether the user is authenticated through QuickFile or a company directory. You can prevent a user from using their credentials to log in to the system.

You can configure a user to be authenticated through an LDAP company directory. First, set up a lightweight directory access protocol (LDAP) server. Then, request that the user login to QuickFile. The user is then added to the user list and is identified as an LDAP user.

When you authenticate users through the LDAP server, they cannot change their QuickFile password through QuickFile. LDAP users must change their password through the company directory.

## Creating or editing a user account

Use QuickFile to add a user to the system. After the user is added, the user receives a New User Registration notice. The user must click the link in the email notice and define a password within seven days. If not, the registration expires. You can reset a user account to allow the user more time to register. After you create a user account, you can modify the account and change any of the settings. Access to administrative tools is limited to Admin users.

### Before you begin

To create a user account:

### Procedure

1. Click **Users** from the menu. The list of current users is displayed.

   The columns list the user name, role, groups the user is assigned to, user type, and status of the user account.
2. Click **Create**.
3. Type the user **Email address**. Type the same address in the **Confirm email address** field.
4. Type the user **Full name**.
5. Click **Create**.

### What to do next

To edit an existing profile, click the user name in the list of users.

## Deleting a user account

You can add a user account or a user account is added when a user registers. Use the **User** page to delete a user account that is no longer needed.

### About this task

To delete a user account:

### Procedure

1. Click **Users** from the menu. The list of current users is displayed.
2. To delete a user, enable the check box next to the user name to modify and click **Delete**.
3. Click **Delete** to confirm the deletion.

   **Attention:** After a user account is deleted, that user cannot log in and activity is no longer available. The user must register to use the system.

## Resetting a user account setup

When you create a user account, a New User Registration notice is sent to the user. To complete the user account setup, the user must click the link in the notice and define a password. The process must be completed within seven days or the user account setup expires.

### Before you begin

If the user setup expires, the administrator can reset the user account. The user is then given seven more days to update the password.

To reset the user account setup:

### Procedure

1. Click **Users** from the menu. The list of current users is displayed.
2. Enable the check box next to the user name to reset.
3. Click **More** > **Reset**.

## Expiring an external user account

System administrators can force an external account to expire before the assigned expiration date.

### About this task

External user accounts expire after a time period. Change the expiration date to disable a user on a different date.

To change the user account expiration:

### Procedure

1. From the **Administration** menu, click **Users**. The list of current users is displayed.
2. Check the user box that you want to modify.
3. Click **More** > **Reset** > **Account Expirations**.
4. Select the new expiration date and click **Save**.

   **Restriction:** The expired user registration is not disabled until the scheduled task named `User` runs. The default schedule is 4 AM each day. To run the task at another time, see "Suspending or resuming a task" on page 66.

## Extending a user account

System administrators define how long an external user account is active in the user account expiration policy.

### About this task

External user accounts expire after a time period. Seven days before account expiration, the user receives an Account Expiration Notification. The user can request an extension by clicking the link in the notification email. When the user requests an extension, you can extend the account.

To extend the user account and assign a new expiration date:

### Procedure

1. From the **Administration** menu, click **Users**. The list of current users is displayed.
2. Select the check box for the user that you want to modify.
3. Click **More** > **Reset** > **Account Expirations**.
4. Select the new expiration date and click **Save**.

   **Restriction:** If the admin user is not defined with a valid email address, expiring external users cannot extend the account from the expiration notification.

## Locking or unlocking a user

Use QuickFile to lock out a user to prevent access to the system. You also can unlock a user that you locked.

### Before you begin

To lock a user or unlock a user:

### Procedure

1. Click **Users** from the menu. The list of current users is displayed.
2. To prevent a user from logging in to QuickFile, enable the check box next to the user name and click **More** > **Lock**.
3. To unlock a user account, enable the check box next to the user name and click **More** > **Unlock**.

## Changing a role assigned to a user

As administrator, you can change the responsibilities that a user is allowed to perform. By default, a user is defined as a basic user. The user can send a file and receive a file but cannot change any policies, environmental settings, or add users. Administrators can perform all of the functions that a user can perform and can also define policies, configure the environment, and add users. Access to administrative tools is limited to Admin users.

### Before you begin

Complete the following steps to change a user role:

### Procedure

1. Click **Users** from the menu.
2. Enable the check box next to the user to modify.
3. Click **More** > **User role** and select the role to assign to the user:
   - Admin
   - User

## Changing a user account authentication type

Configure QuickFile to identify how a user is authenticated. Select QuickFile or LDAP to manage user credentials for each user. Users who are authenticated by LDAP are defined by the LDAP server. LDAP users log in to QuickFile with their LDAP credentials. LDAP users are not required to register with QuickFile.

### Before you begin

The lightweight directory access protocol (LDAP) is an industry-standard Internet Protocol. It stores and accesses user information from an LDAP server. If your company uses LDAP, you can make that data available to QuickFile.

**Restriction:** The Company LDAP option is active only if you establish a connection between QuickFile and your LDAP server.

With an LDAP connection, you can define users and user groups with LDAP and eliminate the requirement to define users in QuickFile.

If you enable LDAP, do not use QuickFile to add and manage user credentials. Use the LDAP tools instead. If a user tries to log in to QuickFile with an expired LDAP password, the user is notified that the password expired. The user or the LDAP administrator must change or reset the password on the LDAP directory. The LDAP directory is created and managed separately from QuickFile.

To change a user authentication type:

### Procedure

1. Click **Users** from the menu. The list of current users is displayed.
2. Enable the box next to the user name to edit and click **More** > **Authentication type** and select the authentication type:
   - Company LDAP - to use LDAP
   - Application - to use QuickFile

   **Attention:** If you switch the authentication type from Company LDAP to Application, the user receives an email with an access code and instructions to set their password in QuickFile.

## User Account Listing field definitions

Use the User Account Listing page to view user information for each defined user.

| Field Name | Description |
|---|---|
| Name | The full name of the user, as provided when the user account was created, or as edited by the user or administrator. Required. |

| Field Name | Description |
| --- | --- |
| Role | Type of user. A User is a regular user who can send and receive files but cannot add users or policies. An Admin can add policies, add and modify users, lock and unlock users, delete users, and change configuration settings. |
| Groups | The QuickFile group to which the user is assigned. The user can be assigned to only 1 group. Admin users cannot be added to a group when you define the user. However, Admin users are added to a default group, if one is defined. |
| Type | Identifies a user as internal or external. An internal user is defined on the domain within the company. An external user is a user outside of the company server. |
| Status | The status of the user account. The following values are valid:<br>• lock<br>• unlock<br>• delete<br>• pending registration<br>• registration expired<br>• departed<br>Departed is a user who is removed from LDAP and later, attempts to log back in to the system. |

## User Account field definitions

Use the User Account page to create and view user information. You can create a user account or view information about an existing account. You can delete a user account. You can change the account type, the user role, and the authentication method. By clicking the name of a user, you can view and edit information on the user Profile page.

| Field Name | Description |
| --- | --- |
| Email address | The email address that is used to send and receive files. Specify this value when you create a user through the Create User dialog. |
| Confirm email address | When you add the user account, retype the email address for verification. Required. |
| Full name | The full name. Required. |

# Chapter 10. Use groups to manage user settings

Create a group and add users to the group to quickly assign similar policies to a group of users.

Be sure to define default policies before you define a group. You can then assign the default policies, including file management, password, and lockout policies to the group. Based on the user requirements, you can create a group and define a custom policy for one or more of the policies. A user can be assigned to only one group.

## Creating a group

You can quickly define what functions a user can perform by creating a group, associating policies with the group, and adding users to the group. As needed, you can edit and delete groups.

### About this task

To create a group and add users and policies to the group:

### Procedure

1. Click **Groups** from the navigation pane.
2. To create a group, click **Create**.
3. Type a name and description for the group.
4. To use this group as the default for all newly registered user, click **Make this the default group for newly registered users**.
5. Click **Next**.
6. To use the default policies, enable **Use the default policies for the group**.
7. To set custom settings for one of the following areas, click **Define a custom policy for this group**. Define settings for the policy definition according to the instructions listed in the following table:

| Policy to customize | Link to procedure |
|---|---|
| Temporary lockout policies | "Setting user lockout policies" on page 61<br><br>**Restriction:** Account expirations cannot be defined at the group level. They are enabled or disabled for all users. |
| Password policies | "Setting a password policy" on page 69 |
| System management policies | "Policies for file transfer expiration and file size" on page 71 |
| User management policies | "Defining users who are allowed to send registration invitations" on page 73<br><br>"Defining file transfer restrictions" on page 72 |

8. Click **Next** to move through the wizard.
9. To add a user to the group, use the following procedure:

a. Select the user in the **Available Users** panel.
b. Click **Add selected users to group** (right arrow) to move the user to the **Selected Users** panel.
c. Click **Next**.

10. On the **Summary** page, validate that all settings are correct and click **Finish**.

## Editing a group

You can modify a group to change information, including users that are assigned to the group and policies that are associated with it.

### About this task

To edit a group, complete the following steps:

### Procedure

1. Click **Groups** from the navigation pane.
2. To edit an existing group, click the group name from the listing.
3. If wanted, modify the name, description, or if this group is applied to newly registered users.
4. To change the policies that are associated with the group, click the **Policies** tab and modify one or more settings:
   - To modify the lockout policy settings, use the procedure, "Setting user lockout policies" on page 61.
   - To modify the file management policy, use the procedure, "Defining file transfer restrictions" on page 72
   - To modify the password policy, use the procedure, "Setting a password policy" on page 69
   - To modify the system management policy, use the procedure, "Policies for file transfer expiration and file size" on page 71
5. To add users to the group, use the following procedure:
   a. Click the **Members** tab.
   b. Select the users in the **Available Users** panel.
   c. Click **Add selected users to group** (right arrow) to move the users to the **Selected Users** panel.
   d. Click **Next**.
6. To remove users from the group, use the following procedure:
   a. Click the **Members** tab.
   b. Select the users in the **Selected Users** panel.
   c. Click **Remove selected users from group** (left arrow) to move the users to the **Available Users** panel.
   d. Click **Next**.
7. On the **Summary** page, validate that all settings are correct and click **Save**.

## Deleting a group

You can delete groups that you no longer need. You can delete multiple groups at one time.

### About this task

To delete a group:

### Procedure

1. Click **Groups** from the navigation pane.
2. Select the groups to delete and click **Delete**.
3. Click **Delete** to confirm the deletion.

## Groups field definitions

The following table lists the fields on the **Groups** page and their definitions:

| Field | Definition |
|---|---|
| Name | Name that is assigned to the group. |
| Description | Description of the group. |
| Make this group the default group for newly registered users | Select this option to use the defined group settings for any new users who are register with QuickFile. |
| Define custom policies for this group | Select this option to define new custom policies for the group. You can define settings for one or more policy types. |
| Policies tab | Click this tab to display the policies that you can define. See the following topics:<br>• "Setting user lockout policies" on page 61 to define a lockout policy<br>• "Setting a password policy" on page 69 to configure a password policy<br>• "Policies for file transfer expiration and file size" on page 71 to configure a file transfer policy<br>• "Defining file transfer restrictions" on page 72 to configure a user policy |
| Members | Click this tab to define the users that are associated with the group. To add users to the group, highlight the users in the **Available Users** panel and click **Add selected users to group** (right arrow). Users in the **Selected Users** panel are members of the group. |
| Summary | The summary page displays the group definition, including the name and description of the group. It also identifies what policies are custom policies, and how many users are in the group definition. |

# Chapter 11. Viewing active users

You can view how many active users are defined in QuickFile. Active users include all users that are defined and are not deleted.

## Before you begin

Active users are all users who are defined in the system. Active users include internal users who are defined in the mail domain and external users who are not defined in the mail domain. It also includes registered users who signed up with QuickFile and unregistered users.

The data is updated when you open the page. To refresh the data, close the page and reopen it.

To view a list of active users, select **Administration** > **System Information**.

# Chapter 12. Performance

Performance of your QuickFile system must be maintained to meet your business requirements.

The performance of your QuickFile system is affected by the following factors:

- Number of active users
- Volume of file transfers
- File size of transfers
- Peak load activity
- Archiving
- Purging
- Logging

Monitor your performance and compare the actual to the criteria set for your business requirements. See the following topics for more information:

- "Collecting and monitoring performance data"
- "Maintaining and improving performance" on page 88

## Collecting and monitoring performance data

Use the **nmon** utility to collect and monitor performance data.

The data that is collected includes processor use, memory use, and run queue information. It also analyzes disk input and output rates, transfers, read/write ratios, and how much free space is available on file systems.

The tool collects and displays important system resource utilization information and dynamically updates it. Type the commands in the procedure on the QuickFile console. You must have ADMIN authority. To move the data collection file to a different remote server, the remote server must have an SSH server that is installed for the **file put** command to work.

Complete the following steps to start the utility in data collection mode and stop it.

1. Type **wizard startNmon.xml** at the command prompt.
2. Provide the name of the output file where data is written.

   The utility starts in the background.
3. To stop the tool, type **wizard stopNmon.xml**.

   **Tip:** It is a good practice to stop an existing **nmon** process before you start another one. Type **file list** to view the contents of `/tmp/userfiles`.
4. After the data is collected, type

   `file put` *`file name protocol://user@host/path`*

   to copy the data that is collected to a location. The variable values are defined in the following table:

*Table 12. Variables for the* **nmon** *utility*

| Variable | Definition |
|---|---|
| file name | Name of the output file that contains data that is created by the collection tool. |
| protocol | Either SCP or FTP. |
| user | User ID that can log in to the remote host. |
| host | Host name or IP address of the remote server where the file is copied. |
| path | Path on the remote host where the file is copied |
| Sample command | **file put quickfile.nmon scp://root@192.168.60.128:/nmon-data/** |

5. If multiple instances of the tool are running, type * to stop all instances.

**Tip:** For more information about the utility and more options, see developerWorks.

# Maintaining and improving performance

There are tasks that you can do that might improve the performance of QuickFile. Performance factors include throughput speed, error rates, and failover recovery.

## About this task

To improve the performance of your QuickFile system:

## Procedure

1. Monitor your current performance. For more information, see "Collecting and monitoring performance data" on page 87.
2. Identify situations that are not occurring satisfactorily. For more information, see Chapter 13, "Viewing a log of system events," on page 89.
3. Adjust the settings for maintenance to tasks according to your system activity. Tasks might need to run more or less frequently. For more information, see
   - "Tasks available to schedule" on page 64
   - "Scheduling maintenance tasks" on page 66
   - "Configuring event purge" on page 67
4. Determine what is causing the delay and correct the situation.
5. Adjust the settings for properties that can affect your performance. For more information, see "Tuning the environment" on page 11.
6. Test your new configuration to see if performance has improved.

# Chapter 13. Viewing a log of system events

As administrator, you can view a log of the events that are generated by QuickFile.

### About this task

You can view a log of events that are generated by QuickFile. You determine the number of events to display per page and sort the listing by event type or date. By default, events are sorted first by date and time and next by event name.

To view system events:

### Procedure

1. Click **Log reports** from the menu.
2. Make sure that the **System logs** tab is selected.
3. To sort the event list by event or event date, click the appropriate heading.
4. If more than one page of events is available in a report, click **Next** to display the next page in a report.
5. To move back to a previous page in the events report, click **Previous**.
6. To view the last page of events, click the last page number in the **Page** listing.
7. To view the first page of events, click the first page number in the **Page** listing.
8. To jump to a specific page, type the page number in the **Jump to page** text box or click the page number in the **Page** listing.

## Event log explanation

System events can be viewed by administrators only and describe the events that occur in QuickFile. Each message uses the code format `CIVxx`*`nnnnT`*, where *nnnn* is a unique message number and *T* is the message type. Refer to the following tables for a description of the message code components and the messages that occur:

| Message Code Component | Description |
|---|---|
| *xx* | The message code prefix. Available prefixes include:<br>• `ST` - storage<br>• `ID` - identity<br>• `MB` - mailbox<br>• `VI` - visibility<br>• `MS` - messaging<br>• `CF` - configuration<br>• `CN` - communication<br>• `SC` - scheduling<br>• `CC` - common components |
| *T* | Message type. Available message types include:<br>• E = error<br>• I = information<br>• W = warning |

## Event code descriptions

The following table identifies the messages created in QuickFile.

| Event | Event Code | Message | Description |
|---|---|---|---|
| User self registered | CIVID1001I | *user* self registered | A user completed the registration form from the login page. The user must click a link in the registration email to complete the process. |
| User registration expired | CIVID1002I | *user* self registration expired | A user completed the registration form from the login page but did not click a link in the registration email to complete the process. |
| User invited | CIVID1003I | *user1* invited *user2* to register | *user1* sent an invitation to another user to register. To complete the invitation, *user 2* must click a link in the email to complete the process. |
| User invitation declined | CIVID1004I | *user* declined to register | A user declined the invitation to register. |
| User created | CIVID1005I | *user* created by administrator | An administrator added a user. The user must click a link in an email to complete the user registration. |
| User register confirmed | CIVID1006I | *user* confirmed registration | A user clicked a link in the registration email to complete the registration. |
| User login | CIVID1007I | *user* logged in | User is logged in. |
| User logout | CIVID1008I | *user* logged out | User is logged out. |
| User password change | CIVID1009I | *user* changed password | User changed their password. |
| User login failed | CIVID1010I | *user* failed to login; forgot password | User was unable to log in because the user provided an invalid password. |
| User AFT enabled | CIVID1011I | *user* enabled Advanced File Transfer | User enabled the Advanced File Transfer option to allow the transfer of large files and to enable pause and resume. |
| User AFT disable | CIVID1012I | *user* disabled Advanced File Transfer | User disabled the Advanced File Transfer option. |
| User locked | CIVID1013I | *user* locked by administrator | User is unable to log in to QuickFile because the administrator locked out the user. |
| User unlocked | CIVID1014I | *user* unlocked by administrator | Administrator unlocked the user. |
| User locked failure | CIVID1015I | *user* locked; repeated login failures | User is unable to log in because the user exceeded the maximum number of failed login attempts set by the administrator. |
| User deleted | CIVID1016I | *user* deleted by administrator | User was deleted from the database by the administrator.<br><br>**Remember:** User records are never removed from the database. They are marked as deleted and the user is prevented from logging in. |
| User profile updated | CIVID1017I | *user* updated profile | User modified their profile. |
| User added to group | CIVID1018I | *user* was added to *groupn* by administrator | The administrator added user to a group definition. The group definition determines the policy that is enforced for all users in the group. |

| Event | Event Code | Message | Description |
|---|---|---|---|
| User removed from group | CIVID1019I | *user* was removed from *groupn* by administrator | The administrator removed user from the group definition. User policy enforced when a user is not part of a group are the default settings. |
| User assigned role | CIVID1020I | *user* assigned the role of *administrator or user* by administrator | The administrator modified the role of the user identified. Available roles include user or administrator. |
| Group created | CIVID1021I | *group* created by administrator | The administrator created a group. |
| Group deleted | CIVID1022I | *group* deleted by administrator | The administrator deleted the group called *group*. |
| Group modified | CIVID1023I | *group* modified by administrator | The administrator modified the group. |
| User forgot password | CIVID1024I | *user* requested a password reset | User requested a password reset, possibly because the user forgot the password. |
| User authorization failed | CIVID1025I | *user* failed to login | User failed to log in because of an incorrect password. |
| File sent | CIVCC1001I | *user1* sent file *f* in package *p* to *user2* | User 1 sent a file called *f* in package *p* to user 2. The file is saved to the server. User 2 can now download the file. |
| File resent | CIVCC1002I | *user1* resent file *f* with package subject *p* to *user2user2* | *user1* resent a file called *f* to *user2*. The file is sent to the same user who received the file on the first transfer. The file is saved on the server. User 2 can now download the file. |
| File forwarded | CIVCC1003I | *user1* forwarded file *f* with package subject *p* to *user2* | *user1* forwarded a package called *p* to a new *user2*. The file is saved on the server. User 2 can now download the file. |
| File downloaded | CIVCC1004I | *user* downloaded a file *f* | A user downloaded a file called *f*. |
| File requested | CIVCC1005I | *user1* requested *user2* to send file with package subject | A user sent a request to another user to send a file. |
| File deleted | CIVCC1006I | *user* deleted file *f* with package subject *p* | A user deleted a file from the file listing. The file is stored on the server and is marked for removal. |
| File expired | CIVCC1007I | *f* with package subject *p* sent to *user2* expired and will be deleted | A file called *f* in package *p* |
| Antivirus scan fail | CIVCC1008E | *f* with package subject *p* from *sending user* contains a virus and will not be transferred. | The named file with the package subject *p* from the sending user contains a virus and will not be transferred. |
| Antivirus scan success | CIVCC1009I | *f* with package subject *p* from *sending user* was successfully scanned for viruses. | The named file with the package subject *p* from the sending user was successfully scanned for viruses and none were found, so the file will be transferred. |
| File removed | CIVCC1010I | *f* in *p* for *user* were abandoned after 7 days and will be removed | The package identified was paused and was not restarted before 7 days elapsed. The package is marked for deletion. |
| File archived | CIVCC1011I | *f* in *p* for *user* were archived | Files for a user were archived. |
| AFT uploaded | CIVCC1012I | *user1* uploaded *n* out of *x* bytes of *f* with package subject *p* to *user2* | *user1* used Advanced File Transfer to send a portion of a file as identified in the *n* out of *x* bytes definition. File is sent to *user2*. |

| Event | Event Code | Message | Description |
|---|---|---|---|
| AFT downloaded | CIVCC1013I | *user1* downloaded *n* out of *x* bytes of *f* with package subject *p* to *user2* | *user1* used Advanced File Transfer to download a portion of a file identified in the *n* out of *x* bytes definition. File is sent to *user2*. |
| File upload exceeded limit | CIVCC1014W | Upload failed because *file1* with package subject exceeds required limit | The file that the user sent is larger than the file size limit and is not transferred. |
| File transfer started | CIVCC1015I | Transfer file *f* with package subject *p* started | The transfer of file *f* started. |
| File transfer ended | CIVCC1016I | Transfer file *f* with package subject *p* ended | The transfer of file *f* ended. |
| Transfer package started | CIVCC1017I | Transfer package with subject *p* started | The transfer of package subject *p* started. |
| Transfer package ended | CIVCC1018I | Transfer package with subject *p* ended | The transfer of package subject *p* ended. |
| Package summary | CIVCC1019I | Summary for package with subject *p* | This is a summary for package subject *p*. |
| Delete recipient | CIVCC1020I | *user* deleted recipient *user* of file *f* with package subject *p* | A user deleted a recipient of file *f* with package subject *p*. |
| File expiration updated | CIVCC1021I | *user* updated expiration date of a file with package subject *p* | A user updated the expiration date of a file in a package |
| DLP detected | CIVCC1022E | *f* with package subject *p* from *user* contains sensitive information (DLP) and will not be transferred | File *f* in package subject *p* from user contains sensitive information (DLP) and the entire package will not be transferred. Remove the sensitive information and resubmit the package. |
| DLP scanned | CIVCC1023I | *f* with package subject *p* from *user* was successfully scanned for sensitive information (DLP) | File *f* in package subject *p* from user was successfully scanned for sensitive information (DLP) and the transfer progressed. |
| Appliance Powered Down | CIVCF1001I | *admin* powered down the server | An administrator is shutting down the server. |
| Appliance Restarted | CIVCF1002I | *admin* restarting the appliance | An administrator restarts the server. |
| Appliance Powering Down | CIVCF1003I | The server is powering down. | The appliance is powering down. |
| Appliance Started | CIVCF1004I | The server has been started | An administrator started the appliance. |
| NFS Configured | CIVCF1005I | Application is configured to use NFS with *nfs configuration* | The application is using NFS. |
| Database Configured | CIVCF1006I | Application is configured to use external database with *db configuration* | The application is using the external database. |
| LDAP Configured | CIVCF1007I | Application is configured to use external directory with *LDAP configuration* | The application is using LDAP. |
| Archive Configured | CIVCF1008I | Application has been configured to use archiving *FileNet* | The application is using *FileNet* to archive files. |

| Event | Event Code | Message | Description |
|---|---|---|---|
| SMTP Configured | CIVCF1009I | Application is configured to use the SMTP server with *SMTP server* | The application is using an SMTP server *SMTP server*. |
| Backup SMTP configured | CIVCF1010I | Application has been configured to use backup SMTP server - *SMTP server* | The application is using a backup SMTP server - *SMTP server*. |
| IP Configured | CIVCF1011I | Application is configured to use IP address with *ip address* | The application is using an IP address. |
| Gateway Configured | CIVCF1012I | Application is configured to use Gateway server with *gateway configuration* | The application is using a Gateway server. |
| Mask Configured | CIVCF1013I | Application has been configured to use subnet mask with *CIDR mask configuration* | The application is using a subnet mask. |
| Fix applied | CIVCF1014I | Fix pack applied to the application *fix pack* | The fix pack *fix pack* is applied to the application. |
| Task policy configured | CIVCF1015I | Application has been configured to use task *task* with initial state *state* and repeat interval *interval* | The application is configured to run maintenance task *task*, starting with *state* and running every *interval*. |
| Antivirus configured | CIVCF1016I | Application has been configured to use *provider name* for antivirus. | The application is configured to use the ICAP provider named *provider name* for antivirus scanning. |
| ICAP server enabled | CIVCF1017I | *admin* successfully enabled ICAP server *server name* | An admin successfully enabled an ICAP server named *server name*. |
| ICAP server disabled | CIVCF1018I | *admin* successfully disabled ICAP server *server name* | An admin successfully disabled an ICAP server named *server name*. |
| DNS server enabled | CIVCF1019I | Application has been configured to use DNS server *server name* | An admin successfully enabled a DNS server named *server name*. |
| ICAP server deleted | CIVCF1020I | *admin* deleted ICAP server *server name* | An admin deleted an ICAP server named *server name*. Scanning by this server is disabled. |
| DNS server deleted | CIVCF1021I | *admin* deleted DNS server *server name* | An admin deleted an DNS server named *server name*. Login management by this server is disabled. |
| NFS Connection Failed | CIVCF1020E | NFS with *nfs configuration* failed to connect | NFS did not successfully connect to the server. |
| Database Connection Failed | CIVCF1021E | External database with *db configuration* failed to connect | The external database did not successfully connect to the server. |
| LDAP Connection Failed | CIVCF1022E | LDAP with *ldap configuration* failed to connect | LDAP did not successfully connect to the server. |
| Archive Connection Failed | CIVCF1023E | Archive with *archive configuration* failed to connect | The archive tool did not successfully connect to the server. |
| DNS Connection Failed | CIVCF1024E | The Gateway server using the *gateway configuration* failed to connect | The gateway server did not successfully connect. |
| SMTP Failed | CIVCF1025E | SMTP server connection failed. | The SMTP server connection failed. |

| Event | Event Code | Message | Description |
|---|---|---|---|
| Fix Pack Failed | CIVCF1026E | Fix pack updates with *update info* failed | The fix pack did not successfully install. |
| No SMTP Server | CIVCF1027E | No SMTP server configured | No SMTP server is configured. |
| SMTP Server Failed | CIVCF1028E | Failed to connect to the SMTP server | The application failed to connect to the SMTP server. |
| Out of Disk Space | CIVCF1029E | Appliance ran out of disk space | The appliance ran out of disk space and therefore, packages can no longer be uploaded. |
| System policy update | CIVCF1029I | *admin* successfully updated policy *policy* | An administrator successfully updated a system policy. |
| System policy enabled | CIVCF1030I | *admin* successfully enabled system policy *policy* | A system policy for *policy* was successfully enabled by a user. The following values for *policy* are possible:<br>• Antivirus scan policy<br>• Data loss prevention policy<br>• Email notification policy<br>• Event retention policy<br>• Expiration notification policy<br>• Password policy<br>• Password reset policy<br>• User expiration policy |
| System policy disabled | CIVCF1031I | *admin* successfully disabled system policy *policy* | A system policy for *policy* was successfully disabled by an administrator. |
| Temp suspend task | CIVSC1001I | Application has temporarily suspended task name *task* | Application has temporarily suspended task name *task*. |
| Temp resume task | CIVSC1002I | Application has temporarily resumed task name *task* | Application has resumed task name *task* that was temporarily suspended. |
| Run now task | CIVSC1003I | *admin* has requested the immediate execution of task name *task* | An administrator requested the immediate execution of task name *task* |
| Internal email domains added | | *admin* added internal email domain *domain name* | An administrator added an internal mail domain named *domain name*. |
| Internal email domains deleted | | *admin* deleted internal email domain *domain name* | An administrator deleted an internal mail domain named *domain name*. |
| SSL Expired | CIVSE1001I | SSL certificate *alias* expired | The SSL certificate expired. Request a new one from your CA. |
| SSL Imported | CIVSE1002I | SSL certificate *alias* imported by *admin* | An administrator imported an SSL certificate. |
| SSL Exported | CIVSE1003I | SSL certificate *alias* exported by *admin* | An administrator exported an SSL certificate. |
| SSL Enabled | CIVSE1004I | SSL enabled | An administrator enabled SSL. |
| SSL Disabled | CIVSE1005I | SSL disabled | An administrator disabled SSL. |
| SSL certificates added | | *admin* added SSL certificate *cert name* | An administrator added an SSL certificate named *cert name*. |

| Event | Event Code | Message | Description |
|---|---|---|---|
| SSL certificates deleted | | *admin* deleted SSL certificate *cert name* | An administrator deleted an SSL certificate named *cert name*. |
| User expirations updated | CIVSE1006I | *user* expirations updated | The user account expiration date changed. |
| User expirations notified | CIVSE1007I | *user* notified of upcoming account expiration | The user is notified that their account expires soon. |
| User expirations processed | CIVSE1008I | *user* accounts expired | The user account expired. |
| Email failed | CIVMS0001E | Email notification for *user* could not be delivered | An email notification for a user could not be delivered. |

# Generating a support log

If Support instructs you to generate a support log, use QuickFile to generate a support log.

## About this task

When you are troubleshooting a problem you experience with QuickFile, Support might ask for you to turn on the support log. QuickFile makes this job easier with Log Reports.

One of the Log Reports tabs gives you the ability to turn on the support log. Using the support log, you can generate logging information and export the information to a file for Support to use. Because of the temporary impact that logging has on system performance, turn on logging only when Support instructs you to do so.

To turn on logging, complete the following procedure:

## Procedure

1. On the Administration tab, click **Log reports** from the menu.
2. Click **Support logs**.
3. Select **Enable support logging**.
4. Select one of the following application logs to view:
   - Application server
   - Database
   - Messaging
   - Operating system
5. If you select **Application server** as the log to view, type the exact log information as instructed by Support. For example:

   ```
   com.ibm.mft.*=ALL
   ```
6. If you select **Database**, provide information in the following fields:
   - **Log severity Level**
   - **Log query plan** - True or False
   - **Log statement text** - True or False

- **Deadlock trace** - True or False

7. If you select **Messaging** as the log type, select one or more of the following fields to define the log levels to view:
   - **trace**
   - **cluster**
   - **defs**
   - **kernel**
   - **dap**
   - **topic**
   - **logger**
8. If you select **Operating system**, select one of the following error levels to log:
   - **Debug**
   - **Info**
   - **Warn**
   - **Error**
   - **Message**
   - **Fatal**
9. After you enable logging, you must cause the events to occur again and be captured in the log. Under direction from Support, re-create the original problem. After you re-create the problem, return to the **Support logs** page.
10. Export the event log to a file, complete the following steps:
    - Select the dump files to export, enable **Java dump** files or **Heap dump** files or both.
    - Click **Export**. A file is downloaded to your computer.
    - Open or save the file as needed.
11. Click **Save**.
12. Send the log files to Support for analysis. From the Administration page, click **Log reports** from the menu.
13. Click **Support logs**.
14. Select **Export**.

### What to do next

After the issue is resolved, return to the **Support logs** page to disable support logging. Otherwise, system performance might be impacted.

## Viewing events that are not in the log

You can use the event log to generate a list of commonly occurring tasks. However, not all events and errors are available in the log. Gather and download all the system logs to obtain all the events.

### Before you begin

Complete the following steps to gather and download all system logs:

### Procedure

1. Type the following url in your browser: `http://`*`ip address`*`:9080/quickfile/rest/admin/mustgather`

2. Type your administrator user ID and password.
3. Save the file that is called `quickfileMustGather.tgz`.
4. Extract the file to view all QuickFile logs.

# Chapter 14. Troubleshooting

When file transfers fail, you perform procedures to identify the cause of the failures and resolve the issues.

## About this task

To troubleshoot issues with QuickFile:

## Procedure

1. Identify the types of transfers that are in failed status.
2. Examine the logs to determine common characteristics of the failed transfers. For more information, see Chapter 13, "Viewing a log of system events," on page 89.
3. You can also obtain events that are not in the logs. For more information, see "Viewing events that are not in the log" on page 96.
4. Visit the QuickFile Support portal.
5. Take actions to remedy the conditions that cause failed transfers.
6. If you need additional help in resolving issues, generate a log to send to IBM Support. For more information, see "Generating a support log" on page 95.

# Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

*IBM Director of Licensing*

*IBM Corporation*

*North Castle Drive*

*Armonk, NY 10504-1785*

*U.S.A.*

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

*Intellectual Property Licensing*

*Legal and Intellectual Property Law*

*IBM Japan Ltd.*

*19-21, Nihonbashi-Hakozakicho, Chuo-ku*

*Tokyo 103-8510, Japan*

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:**
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be

incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

*IBM Corporation*

*J46A/G4*

*555 Bailey Avenue*

*San Jose, CA 95141-1003*

*U.S.A.*

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© IBM 2014. Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 2014.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

## Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium and the Ultrium Logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Connect Control Center®, Connect:Direct®, Connect:Enterprise, Gentran®, Gentran®:Basic®, Gentran:Control®, Gentran:Director®, Gentran:Plus®, Gentran:Realtime®, Gentran:Server®, Gentran:Viewpoint®, Sterling Commerce™, Sterling Information Broker®, and Sterling Integrator® are trademarks or registered trademarks of Sterling Commerce®, Inc., an IBM Company.

Other company, product, and service names may be trademarks or service marks of others.

# Index

# K



# L



# M



# N



# O



# P



# Q



# R



# S



# T

# U



# V

Product Number: 5725-F81

Printed in USA