Configuring Fiery server settings

Access Configure

After you start the Fiery server for the first time, or install system software, you must set up the Fiery server. If you do not, default settings are used. Make sure that the settings are appropriate for your printing environment. If your network or printing environment changes, you may need to adjust your settings.

When you use proxy servers with the default web browser, you may not be able to start Configure from Command WorkStation. Register the Fiery server IP address as an exception in the default browser settings. Verify your default browser connection settings and adjust them accordingly.

You can set up the Fiery server from a client computer using Configure, which you can access from the following locations:

- Command WorkStation
- WebTools (with a supported Internet browser)

Access Configure from Command WorkStation

1. From Command WorkStation, connect to the desired Fiery server and log in as Administrator.
2. Do one of the following to start Configure:
   - In Device Center, select General Info, then click Configure in the lower right corner.
   - In the Server menu, click Configure.
3. From Configure, change current Fiery server setup options.

Access Configure from WebTools

Use Configure to set up the Fiery server. Setup is required the first time the Fiery server is turned on or after system software is installed. You also use Configure to specify information about the network environment and printing preferences for jobs that users send to the Fiery server.

1. Open an Internet browser and type the IP address of the Fiery server.
   If you have disabled Web services from the printer control panel, you must type https://IP address.
2. In WebTools, click the Configure tab.

   Note: When you start Configure, the browser may display a security certificate error. You can safely proceed despite the error.

22 August 2023

3 Log on with Administrator privileges.

Setting up the server

Use Configure to set up the Fiery server. Setup is required the first time the Fiery server is turned on or after system software is installed. You also use Configure to specify information about the network environment and printing preferences for jobs that users send to the Fiery server.

Note: Some Configure options may not be supported by your Fiery server.

For information about Configure options not discussed in this Help, see *Configuration and Setup*, which is part of the user documentation set.

Configuration workflow

With Configure, you can view and maintain Fiery server settings that are necessary for printing and processing jobs over the network.

1 To view server configuration settings, in Command WorkStation, connect to the desired Fiery server and click Device Center > General > Server Configuration.

2 To change the settings, click Configure in the lower-right corner.
For alternative ways to access Configure, see Access Configure on page 1.

3 From Configure, navigate to the setting that you want to change.

4 After you have changed the setting for an option, click Cancel or Save.

5 When you have finished making your changes, reboot the Fiery server.

Note: The changes you make are not applied until the Fiery server reboots.

Users and Groups

You can define privileges for the users who access the Fiery server by assigning them to groups. Several groups are provided by default. All users in a group have the same privileges.

You can view detailed information about users and groups from Configure > User Accounts.

In addition to assigning to a group the users that you have created, you can add users from your organization's global address list. To do so, you must first enable LDAP services on the Fiery server.

Create new users

If users are not in the global address list or contact list, you can create them manually. Any name that appears in the contact list can become a user that you assign to a group.

The Administrators and Operators groups have a default user named "Administrator" or "Operator," respectively.

1 From Configure, select User Accounts.

2 Click the Fiery Contact List button.

3 In the Fiery Contact List dialog box, click the Add User button.

4 In the Create User dialog box, specify the required information. Click Create.

5 Click Close.

Add users to existing groups

You can add existing users to an existing group, or you can create users and add them to the existing group. You can add users to as many groups as you want.

Creating a user account does not assign any privileges to that user until you add the user to a group.

1 From Configure, select User Accounts.

2 Select the group to which you want to add users.

3 Click Assign Users.

4 Assign the user to groups as required, using any of the following approaches:

- To create a new user and assign them to a group, select Create New User & Assign from the drop-down list, type the appropriate information in the Create User dialog box, then click Save.
- To assign an existing user account to a group, select Add from Contact List. In the Assign Users dialog, enter the account name under Users of Fiery Contact List, and press return, or select the account if listed and click Add Users.
- To assign a SSO user account to a group, select Add from Azure AD. In the Assign Users dialog, select SSO Users List and log in. If the user already has an active Azure session, WebTools will fetch the list of users from Azure. If not, the user will be prompted to enter Azure login credentials. Search the SSO user from the list, select the account if listed, and click Add Users.
- To assign a user from the Global Address List, select Add from Global Address List. If LDAP is configured and enabled, this list contains names from your organization's corporate database. If the Configure LDAP Settings button displays, click the button to configure the LDAP settings to work with Command WorkStation.

5 Click Close when you have finished adding user accounts to groups.

Remove users from groups

You can remove a user from a group. Any jobs that the user has already sent to the Fiery server are still processed, and the Job Log retains the name of the user with relevant job information.

After you remove a user from a group, the user still remains in the Fiery Contact List.

Note: You cannot remove the default users named "Administrator" or "Operator."

1 From Configure, select User Accounts.

2 Select the group in which the user exists.

3 Move the cursor over the name of the user you want to remove from the group.
Notice that the Edit and Delete icons are displayed.

4 Click the Delete icon.
The user is deleted from the group, but not from the Fiery Contact List.

Change user attributes

You can change user attributes, such as the user password and email address. If the user is already logged in, your changes affect the user when the user logs out and logs in again.

To change the default Administrator and Operator passwords, you can use the following procedure or configure a new password.

1. From Configure, select User Accounts.
2. Click the Fiery Contact List button.
3. Move the cursor over the name of a user.
   Notice that the Edit icon is displayed.
4. Click the Edit icon. In the Edit User dialog box, edit user attributes and click Save.

Change group privileges

1. From Configure, select User Accounts.
2. Move the cursor over the name of a group.
   Notice that the Edit icon displays.
3. Click the Edit icon. In the Edit Group dialog box, select or clear privileges and click Save.

   Note: These privileges may not be supported on all Fiery servers.

   - Calibration - Allows members of this group to calibrate the Fiery server. For the default groups, only Administrator and Operator groups have this privilege.
   - Create Server Presets - Allows members of this group to save a set of print options that users can select for their job.
   - Manage Workflows - Allows members of this group to create, edit, and delete Server Presets and virtual printers.
   - Edit jobs - Allows members to edit jobs in the Held or Printed queues.

Delete users

You can delete a user from the Fiery server completely. Any jobs that the user has already sent to the Fiery server are still processed, and the Job Log retains the name of the user with relevant job information.

Note: You cannot delete the default users named Administrator or Operator, and you cannot delete the Administrators or Operators group.

1. From Configure, select User Accounts.

2 To delete a user from the Fiery server completely, do the following:

a) Click the Fiery Contact List button.

b) In the Fiery Contact List dialog box, move the cursor over the name of the user you want to delete.
Notice that the Edit and Delete icons display.

Note: The Delete icon only displays if you are allowed to delete the user.

c) Click the Delete icon.
The user is deleted from the Fiery server completely.

d) Click Close.

Single Sign-On (SSO)

The Fiery server supports the OpenID Connect protocol for cloud-based, Single-Sign-On (SSO) user authentication with Microsoft's Azure Active Directory (AAD). Users log in to the Fiery server using their existing AAD credentials.

The SSO authentication method supports Multi-Factor Authentication (MFA). SSO helps establish the user's identity by verifying the necessary information. With SSO, users with the appropriate access can log in to the Fiery server without having to authenticate every time. SSO ensures a secure login because the Fiery server does not store any user passwords locally.

The Fiery server must not be connected to a proxy server. It must be directly connected to the internet. You must also ensure the availability of the internet and an active Microsoft Azure account.

Register a new application in Azure AD

You must register an application in the Azure AD tenant where the user accounts reside.

1 Log in to the Azure account.

2 Navigate to Azure Active Directory > Manage > App registrations > New registration.

3 Enter the details in the Register an application page.
You can copy the Redirect URL from WebTools > Configure > Network > Single Sign-On. The app will be registered even if you do not add the Redirect URL at this time. You can add the Redirect URL later.

4 Click Register.

Add the Redirect URL after registering an application

1 Click Add a Redirect URL in the overview section.

2 Click Add a platform under Platform configurations in the pane on the right side.

3 Select Mobile and desktop applications.

4 Add the Redirect URL in Custom redirect URLs.

5 Click Configure.

Grant API permission

After registering the application, you must grant the API permission for the application to read the information from Azure AD.

1. Log in to the Azure account and navigate to Manage > API permissions > Add a permission.
2. In the Request API permissions page, select Microsoft Graph > Delegated permissions.
3. In the search bar, type "directory" and select the Directory.Read.All checkbox.
4. Click Add permissions.
   The request must be granted by the administrator.

Make SSO available as a login method

You can allow SSO users to log in to Command WorkStation and WebTools

To see the authentication messages in a different language, change your browser language.

1. In Configure > Network > Single Sign-On (SSO), select Enable SSO.
2. Copy this information from the Azure account and paste it in the Single Sign-On window
   - OpenID Connect metadata document
   - Directory (Tenant) ID
   - Application (Client) ID

   The Directory (Tenant) ID and Application (Client) ID are available in the Overview section of the registered app. The OpenID Connect metadata document URL is visible when you click Endpoints in the same section.
3. Copy the Redirect URL and add it in the Authentication section of the registered app in Azure.

   The Redirect URL is pre-generated and contains the name of the Fiery server. If the host name changes, you must restart the Fiery server and add the new Redirect URL in Authentication section of the registered app in Azure.

   The Fiery server cannot have the same hostname as another Fiery server in the same intranet.
4. Click Save.
5. To validate the details, click Validate.
   The pop-up blocker in your web browser must be turned off.
6. Click Advanced in the warning page and click Accept the Risk and Continue.

   Depending on your web browser, the option names may be different.

   If the details are correct, the validation will be completed in 180 seconds. If the validation times out, restart the procedure for authentication.

Add User Accounts in Configure (WebTool)

After the SSO configuration, the administrator can add users with specific user privileges to groups .

1. Log in to Configure > User Accounts > Assign Users > Add from Azure AD.

2 In the Assign Users window, click Log In.

If you already have an active Azure session, WebTools will fetch the list of users from Azure. If not, you will be prompted to enter Azure login credentials.

3 Select the user name that you want to add and click the right arrow.

Server setup

You can perform tasks such as specifying general settings, setting job options, configuring Administrator and Operator passwords, managing the Job Log, and specifying JDF settings.

Set the Fiery server name

You can specify the name of the Fiery server and configure other general settings.

1 From Configure, choose Fiery Server > Server Name.

2 Type a name for the Fiery server as you want it to appear on the network.

Note: If you have more than one Fiery server, do not assign them the same name.

Configure language and regional settings

When you select a language, regional settings (except time and date) are configured automatically based on your selection. You can also manually change any of the settings as needed.

1 From Configure, choose Fiery Server > Regional Settings.

2 In Server Language, select a language.

3 If you want to change the regional settings individually (such as only Measurement Units), change the settings as needed.

4 Save your changes.

Note: The Fiery server must reboot to apply the language change.

Configure date and time manually

The Regional Settings feature enables you to manually set a time zone and daylight savings settings.

1 From Configure, choose Fiery Server > Regional Settings.

2 Specify the date and time.

Configure date and time automatically

You can use an automatic date and time mechanism by selecting a time server and a polling interval.

1 From Configure, choose Fiery Server > Regional Settings.

2 Select Set Date and Time Automatically and then click the Manage link.

3 Select a time server and polling interval.

The polling interval determines how frequently the Fiery server receives updates from the time server.

Set job options

You can configure settings for options that affect all jobs, such as whether to enable the Printed queue.

1 From Configure, select Job Management > Printed Queue, then select the Save printed jobs check box.

If this option is enabled, you can reprint jobs from the Printed queue without resending them to the Fiery server. If this option is not enabled, jobs are deleted from the Fiery server hard disk after they are printed.

2 In the Jobs Saved in Printed Queue field, type the number of jobs you want to be saved in the Printed queue.

Note: This option is available only if you enable the Printed queue. Be aware that jobs saved in the Printed queue occupy space on the Fiery server hard disk.

3 The Fiery server generates a thumbnail preview of the first page of a job as it is imported. This preview is always generated for spooled jobs, and there is no option to turn off this behavior.

4 To configure the Fiery server to begin processing (RIPping) large jobs before they are done spooling, select Job Management then select the RIP while Receive check box.

Consider these points before enabling this option:

- PDF and VDP jobs are not supported with RIP While Receive because these jobs must spool completely before they are processed.
- Enabling RIP While Receive may cause some jobs to print out of the order in which they were received over the network.
- Depending on the network environment and the speed of the client computer submitting the job to the Fiery server, enabling RIP While Receive can monopolize Fiery server resources for a long time, preventing smaller and/or faster jobs from "skipping ahead" and processing while the RIP While Receive job is still spooling.

5 To control PS to PDF conversion with a job options file, select Job Management > PS to PDF conversion.

6 Save your changes.

Configure Administrator and Operator passwords

You can set the default Administrator and Operator passwords. By default, the Administrator password is set on the Fiery server, but the Operator password is not. Change the Administrator password to protect the Fiery server from unauthorized changes.

Note: Keep track of the passwords that you set.

For more information about passwords, see *Configuration and Setup*, which is part of the user documentation set.

1 From Configure, choose Security.

2 Choose one of the following:

- Administrator Password
- Operator Password

3 Enter and confirm a new password.

4 Save your changes.

Download system logs

You can download the system logs from Configure. These logs are saved as a ZIP file to your computer and can be sent to Technical Support for troubleshooting purposes.

1 In Configure, click Fiery Server > System Logs.

2 Click Download.

Manage the Job Log

The Job Log is a file saved on the Fiery server. It lists all the jobs processed by the Fiery server from the time the Job Log was last cleared or the Fiery server software was reinstalled.

Each Job Log entry includes the user name, document name, print time and date, and number of pages.

1 From Configure, choose Fiery Server > Job Log.

2 To configure the Fiery server to automatically export the Job Log, select Enable Auto Export Job Logs.

If you select this option, specify a date and time for the export to occur. The Job Log is exported as a CSV (Comma Separated Values) file.

3 To ensure that the Job Log is cleared automatically after it is exported, select Clear job log after exporting.

Note: The Job Log is cleared even if the export was unsuccessful. Do not select this option if you are using the Job Log as critical accounting information. In this case, we recommend that you ensure that the Job Log is saved successfully, and then clear it from the Fiery server.

4 To export the Job Log via SMB, select SMB and provide the required information. Click Validate to make sure the SMB information is entered correctly.

JDF Settings

JDF (Job Definition Format) technology is an XML-based open industry standard for job tickets. It simplifies the information exchange among different graphic arts applications and systems.

Fiery JDF allows submission of JDF jobs to a Fiery server from applications that allow creation of JDF tickets.

Use Configure to specify JDF settings and to view the Fiery JDF version, the JDF Device ID, and the JMF URL.

For more information about JDF and JMF, see *Fiery Command WorkStation Help*.

1 From Configure, choose Job Submission > JDF Settings.

2 Select Enable JDF.

3 If a virtual printer is configured for the Fiery server, select one from the Use Job Settings from Virtual Printer option.

Note: Specify this option only if it applies to your specific workflow.

4 Specify a default print queue action from Job action.

5 Select Override JDF job with the above settings, if you want to override the settings specified in the JDF ticket.

6 The JMF (job messaging format) URL section displays read-only information about the Fiery server, which you can use to set up JDF workflows.

7 Specify how you want the JDF jobs closed once they are printed.

8 Specify the items required for closing a JDF job. The items you select here must be filled out before the job can close automatically or manually.

9 Specify the network paths where the Fiery server searches for common resources.

The Fiery server searches these network paths in the order that you specify until it finds the necessary objects. When you type a path, the Fiery server does not verify whether it exists on the network.

Note: Inform users of these paths so that their jobs can access the resources.

10 Save your changes.

Specify contact information

You can specify the contact information for people who provide support for the Fiery server and print device.

1 From Configure, choose Fiery Server and then choose either Fiery Support Contact Information or Printer Support Contact Information.

2 Type contact information into the available fields.

Note: The contact information you enter here also displays in WebTools and in Command WorkStation, in Device Center.

3 Save your changes.

Network setup

Add the Fiery server to your network.

Enter network addresses and names to be used by computers, servers, and the Fiery server when they communicate with each other. Make sure that the Fiery server is connected to a functioning network so that it can query the network for the appropriate information.

Configure Ethernet speed

Specify the speed of the network to which the Fiery server is attached. You can use the Auto Detect feature if you do not know the speed.

1 From Configure, choose Network > Ethernet Speed.

2 Select the speed of the network to which the Fiery server is attached.

If your network environment is mixed or you do not know the network speed, select the Auto (10/100/1000) option.

3 Save your changes.

Configure LDAP

If your Fiery server supports this option, you can configure the Fiery server to communicate with corporate information servers at your organization by means of the LDAP protocol. Fiery server can access lists of email addresses for certain features.

Note: The time difference between the LDAP server and the System Time of the Fiery server (Server > General > Date and Time) must be five minutes or less.

1. From Configure, choose Network > LDAP.
2. In the LDAP Configuration window, select the Enable LDAP check box.
3. Type the name or IP address of the LDAP server.

   The LDAP server IP address and host name must be registered on the DNS server.
4. Type the port number for communicating to the LDAP server.
5. To require secure communication, select Secure Communication (TLS).
6. If authentication is required, select Authentication required and then specify the type of authentication.
7. Type the user name and password for connecting to the LDAP server.
8. If you selected GSSAPI as the authentication type, type the domain name for the LDAP server in the Domain field.
9. In Search Base, type the location where the Fiery server searches to locate the LDAP server. To verify the search base location, click the Validate button at the bottom of the screen.
10. In the Maximum Entries field, type the maximum number of entries that the Fiery server accepts from the LDAP server.
11. In the Search Timeout field, specify the maximum amount of time that the Fiery server spends in attempting to communicate with the LDAP server.
12. Save your changes.

Configure Web services and IPP printing

Enabling Web services allows users to use WebTools.

TCP/IP must be enabled on the Fiery server and user computers. Each computer must also have a Java-enabled Web browser installed and a valid IP address or DNS host name.

After enabling Web services, you can enable Internet Printing Protocol (IPP). Not all models of Fiery serversupport IPP printing.

For information about browser and computer requirements, see *Configuration and Setup*. For information about setting up user computers to use IPP printing, see *Printing*. These documents are part of the user documentation set.

1. From Configure, click Job Submission and select IPP.
2. Save your changes.

Configure SNMP

Enable SNMP to allow remote access to Configure and other Fiery server features.

1 From Configure, choose Network > SNMP.

2 Select Enable SNMP.

3 To restore the Fiery server to its original SNMP settings, click the Restore button.

Note: If SNMP settings have been changed since you loaded the SNMP page, you must click Restore before you make changes.

4 From the Security Level list, select one of the following:

- Minimum - Corresponds to functionality in SNMP version 1.
- Medium - Offers more security for SNMP version 3.
- Maximum - Most secure setting for SNMP version 3.

5 Type the names for Read Community and Write Community.

6 To specify a user name that does not require authentication or encryption with the SNMP server, type the name in the Unsecure User Name field.

7 To specify a user name that requires authentication or encryption with the SNMP server, type the name in the Secure User Name field, and specify the following information:

- User Authentication Type
- User Authentication Password - the password for reading MIB values based on the secure user name
- User Privacy Type - type of encryption (DES or None)
- User Privacy Password

8 Save your changes.

Configuring protocols

When you specify TCP/IP settings, you can assign addresses automatically from a DHCP or BOOTP server.

If you use this approach, make sure that the appropriate server is running before configuring the settings for TCP/IP for Ethernet, DNS, WINS Server, security, IPsec, or certificates.

Configure TCP/IP for Ethernet

You can specify that the Fiery server obtains its IP address automatically or set the address manually.

Note: The Fiery server stores assigned IP addresses, even if you disable TCP/IP later. If you must assign the Fiery server IP address to another device, first set the Fiery server address to the loopback address (127.0.0.1).

The Fiery server requires a unique, valid IP address. You can specify that the Fiery server obtains its IP address automatically or set the address manually. If you allow the Fiery server to obtain the IP address automatically, it also obtains the gateway address automatically.

If you want to set other kinds of IP addresses automatically, such as for a DNS or WINS server, you must allow the Fiery server to obtain its own IP address automatically.

Allow the Fiery server to obtain its TCP/IP address automatically

You can have the Fiery server obtain its IP address, subnet mask, and default gateway address automatically.

1. From Configure, choose Network > IPv4 Address.
2. Set Configure IP Address to Automatic.
3. Choose whether to configure the DNS Server and the WINS Server automatically or manually.
4. Save your changes.
5. If your network uses IPv6 addresses, choose Network > IPv6 Address and select Enable IPv6 Address.

   Note: IPv4 must be enabled for IPv6 to work.
6. Save your changes.

Set TCP/IP addresses for the Fiery server manually

To set TCP/IP addresses manually, you must specify the IP address, subnet mask, and default gateway address.

1. From Configure, choose Network > IPv4 Address.
2. Set Configure IP Address to Manual.
3. Type the IP address, subnet mask, and default gateway address in the respective fields.
4. Choose whether to configure the DNS Server and the WINS Server automatically or manually.
5. Save your changes.
6. If your network uses IPv6 addresses, select Network > IPv6 Address and select Enable IPv6 Address.

   Note: IPv6 requires that IPv4 is already enabled.
7. Save your changes.

Configure DNS

Configure DNS settings to allow the Fiery server to resolve a name to an IP address.

To allow the Fiery server to obtain a DNS address automatically, you must first allow the Fiery server to obtain its own IP address automatically.

1. From Configure, choose Network > IPv4 Address.
2. Select Configure DNS Server and then choose Automatic or Manual.
3. If you select Manual, type the IP address for the primary and secondary DNS servers, and the DNS suffix (domain name).
4. Save your changes.

Configure WINS server (name resolution)

You can specify whether to configure a WINS server automatically or manually The WINS server allows users to access network resources by name instead of IP address.

To allow the Fiery server to configure the WINS server automatically, the Fiery server IP address must also be configured automatically.

1 From Configure, choose Network > IPv4 Address.

2 Next to Configure WINS Server, select Automatic or Manual.

3 If you selected Manual, then type the IP address of the Fiery server.

The name appears on the network when users access the Fiery server through SMB (Server Message Block). This name is the same name as the Fiery server.

4 Save your changes.

Control ports and IP addresses

To control connections to the Fiery server, you can allow communication through specific IP ports, or you can restrict a range of IP addresses.

Allow communication through specific IP ports

To restrict unauthorized connections to the Fiery server, you can restrict network activity to specific ports. Commands or jobs sent from unauthorized ports are ignored by the Fiery server.

1 From Configure, choose Security > TCP/IP Port Filtering.

2 Select Enable TCP/IP Port Filter and specify the ports to enable.

Select only the ports that you want to authorize on the Fiery server.

3 Save your changes.

To enable Remote Desktop access on the Fiery server, make sure that port 3389 is enabled, and that the Remote Desktop option (in the Fiery Server section) is enabled.

Note: Not every Fiery server supports the port 3389 option.

Allow or restrict a range of IP addresses

Restrict unauthorized connections to the Fiery server by defining the IP addresses to accept or deny.

You can deny all IP addresses by default except for ones that you specifically accept, or accept all IP addresses by default except for the ones that you specifically deny. You can specify multiple ranges or IP addresses to accept or deny. Commands or jobs sent from unauthorized IP addresses are ignored by the Fiery server. If you deny IP addresses by default and do not specify valid IP addresses to accept, all network communication to the Fiery server is disabled.

1 From Configure, choose Security > IP Address Filtering.

2. To allow IPv4 address filtering, select the IPv4 Address Filtering check box, indicate whether the Default Filter Policy for IPv4 should be to accept IP addresses except for the ones that you deny, or to deny IP addresses except for the ones that you accept, and click Add IPv4 Address Filtering to specify the IP address range and whether you want to accept or deny the range. You can add multiple ranges.
3. To allow IPv6 address filtering, select IPv6 Address Filtering check box, indicate whether the Default Filter Policy for IPv6 should be to accept IP addresses except for the ones that you deny, or to deny IP addresses except for the ones that you accept, and click Add IPv6Address Filtering to specify an IP address and prefix length, and whether you want to accept or deny this address. You can add multiple IP addresses.
4. Save your changes.

Configure IPsec (Internet Protocol Security)

If users' computers support IPsec, you can enable the Fiery server to accept encrypted communications from users.

1. From Configure, choose Security > IPSpec.
2. Select Enable IPsec.
3. To define the preshared key, type it in the Preshared key box.

   If you define the preshared key, all incoming communication that uses IPsec must contain this key.
4. Save your changes.

Manage certificates

The Fiery server requires a secure connection between user computers and components of the Fiery server. HTTPS over TLS encrypts communications between the two end points. HTTPS is required for a connection to the Fiery server from WebTools. These communications are encrypted with TLS 1.2 and 1.3.

The Fiery server allows the administrator to manage the certificates used during TLS communications (X.509 certificate format encoded in Base64). The Fiery server supports RSA certificates with 4096, 3072, and 2048-bit key length.

You can manage certificates in these ways:

- Create self-signed digital certificates.
- Add a certificate and its corresponding private key for the Fiery server.
- Add, browse, view, and remove certificates from a trusted certificate authority.

Note: Because self-signed certificates are not secure, you must use a certificate from a trusted Certificate Authority (CA).

After you obtain a certificate signed by a trusted Certificate Authority, you can upload the certificate to the Fiery server in Configure.

Add a certificate or private key

When you add a certificate or private key, you specify its location.

1. To view information about a certificate, hover the mouse over the certificate name then click the eye icon. You can also delete the certificate by clicking the trash can icon.
2. From Configure, choose Security > Trusted Certificates.

3 Click Add.

4 Click Browse to select the file and then click Add.

Assign a certificate to the Web server portion of the Fiery server

You can assign or reassign a certificate used by the Web server.

1 From Configure, choose Security > Server Certificate.

2 Click Create Self Signed Certificate.

3 Specify and save your certificate information.

4 To change the certificate used by the Web server, select the certificate, click Change Certificate, and then specify the location of the certificate or private key.

Delete an assigned certificate

You can delete an assigned certificate.

1 From Configure, choose Security > Trusted Certificates.

2 Hover the cursor over the certificate you want to delete.
Notice the Delete icon (trash can) is displayed.

3 Click the Delete icon.

Configure security options

The Fiery server provides many tools to manage security, such as selecting a pre-defined security profile or encrypting user data.

Configure PostScript security

PostScript security restricts access to the software, fonts, color files, and jobs on the Fiery server.
To install fonts using a PostScript-based font downloader tool, clear this option.

1 From Configure, choose Security.

2 Select the checkbox for PostScript Security.

Select a security profile

Fiery Security profiles give you quick access to settings that let you safeguard your Fiery server.

1 From Configure, choose Security > Security Profiles.

2 Click the Select button at the bottom of the column for Standard or High.

The profiles are displayed in a columnar layout.

- Standard: the default security setting
- High: allows the Fiery server to be even more secure and enables the most commonly used security features
- Current: a read-only summary of current security settings

3 Click Save.

Some setup options have additional sub-options, which are not shown in the Security Profiles window. The security profile allows you to set the main (high-level) setting on or off. If there are sub-options, they will remain with default settings. You can configure the sub-options after you select a profile and save your choice.

Collect security events

To help you with compliance requirements at your organization, the Fiery server collects security-related events, which are saved to the Security Audit Log.

Logs are in a format supported by common SIEM log collection and analysis solutions.

The events are in JSON format. You can read events without Fiery, LLC intervention.

1 From Configure, choose Security > Security Audit Log.

2 Select Enable Security Audit Log.

3 To view the events that have been collected, click Download.
The log is provided as a ZIP file.

4 Extract fieryauditlog.evtx and open it in Windows Event Viewer

Security events are retained based on allocated disk storage capacity. When the log size reaches the maximum storage limit (400MB), older events are removed automatically.

Configure printer settings

You can publish print connections and set other settings that affect job processing.

1 In Job Submission > Queues, select the print connections to publish on the Fiery server

- Publish Press Queue - The standard Fiery server queue where jobs are processed and printed in the order in which they are received. On your Fiery server, this option may have a different name or may not be available because the queue is always enabled.
- Publish Hold Queue - The storage area for printing jobs later from the job management tools.
- Publish Font Queue - Select this to download fonts. You must also disable PostScript Security (Security > PostScript Security).

2 To allow jobs to be submitted using Fiery Hot Folders, select Job Submission then select the Fiery Hot Folders check box.

3 Save your changes.

Configure RIP settings

Specify settings that determine how files are processed by the Fiery server.

Adobe PDF Print Engine (APPE)

The Fiery server always uses the Adobe PDF Print Engine (APPE) to process and render PDF jobs without the need to convert them to PostScript. Although there is an option for this in Configure, it is always on.

Configure PostScript settings

You can configure settings that affect PostScript jobs. These settings affect jobs for which users have not specified a setting.

Some combinations of settings may not be appropriate (for example, specifying duplex printing on transparencies). If you specify an inappropriate combination of settings, no error message appears.

1. From Configure, choose RIP > PS settings.
2. Specify settings for the options.
3. Save your changes.

For information about PostScript settings, see *Configuration and Setup*, which is part of the user documentation set.

Configure VDP settings

You can specify the number of records to pre-parse for FreeForm jobs and the network locations (paths) for objects used by variable data printing (VDP).

1. From Configure, choose RIP > VDP.
2. If users will apply imposition or duplex printing to a FreeForm 1 job or FreeForm Create job, select the length of the record:
   - Job - Defines the record boundary as the entire job.
   - FreeForm Master - Defines the record boundary as the length of the FreeForm master.
3. Specify the number of records to examine while a job is spooling.

   If you type a number, the Fiery server examines that number of records as a sample for determining whether the record length is consistent among records. If the records in this sample have the same length, the Fiery server assumes all records in the job have the same length.

   If the Fiery server detects that any of the records have a different length (whether you specify All Records or a sample number), the Fiery server examines all records when necessary for processing or imposition purposes. If the Fiery server does not detect any different lengths in the sample records at spool time, but later detects a subsequent record with a different length, the user is prompted for further action.
4. Click Add to specify the network paths where the Fiery server searches for common objects.

5 In the window that appears, type the path name.

When typing the path name, use the format of a mapped drive (for example, Z:\folder) or a UNC (for example, \\computer name\folder).

6 If the path is located on a computer that requires authentication, select Remote Server Authentication, and then enter the appropriate user name and password.

7 Click OK.

8 To add more paths, click Add and repeat these steps.

9 Save your changes.

HyperRIP Mode

HyperRIP maximizes performance for print jobs by processing print jobs simultaneously. This feature is most useful when print jobs are typically longer than one or two pages.

To access HyperRIP Mode, choose Configure > RIP > HyperRIP Mode.

- Select Auto to allow the Fiery server to select the mode for the most efficient processing of jobs.
- If jobs are typically less than 10-20 pages, select Multiple jobs to process multiple print jobs simultaneously.
- If jobs are typically longer than 10-20 pages, select Single job to split individual jobs into sections that are processed simultaneously.

Note: The most efficient selection depends upon the number and type of jobs being processed and printed. For greatest efficiency, we recommend comparing the output rate for each selection during a typical mix of processing and printing jobs.

Distributed RIP

With the appropriate license, the Fiery server can process jobs on multiple blades. Multiple complex jobs can be processed fast and in parallel ensuring that the backend print pipeline is always full. When the jobs arrive at the Fiery server, they are distributed to the blades for processing in order to maximize throughput.

Distributed RIP maintains all the existing functionality of the Fiery server and is compatible with all existing Fiery applications.

Hardware requirements

The Distributed RIP should be able to run Fiery XB blades with minimum 64 GB RAM. There are no specific requirements for CPU or disk drive.

HyperRIP

Each Distributed RIP can run HyperRIP on it. However, the HyperRIP option in Configure is unavailable when Distributed RIP is active. Instead, this distribution of job processing occurs automatically.

- Jobs are processed among blades as in Job parallel mode. Each blade can process a different job at the same time.
- Within each blade, jobs are processed as if in Page parallel mode.

Even with Distributed RIP, Band parallel mode is on all the time (if the Fiery server is configured for Band parallel mode). Band parallel mode does not have a Configure option. It processes only PDFs of one or two pages, and APPE must be enabled.

Fonts

The Fonts management window lists the fonts resident on the Fiery server. You can also print the font list to a local printer.

Manage fonts on the Fiery server

You can add, update, and delete fonts, as well as print a font list.

In Configure, make these settings:

Enable Job Submission > Queues > Publish Font Queue. For security reasons, enable the Font Queue only while installing fonts.

For PostScript fonts, disable Security > PostScript Security.

Note: All Japanese fonts resident on the server or downloaded by a supported application are locked. Japanese fonts downloaded to the Fiery server can only be deleted by the installing application.

1 Open Device Center in one of the following ways:

- Click the More icon (three vertical dots) next to the server name in the Servers pane.
- Double-click the server name in the Servers pane.
- Click Server > Device Center.
- Right-click the server name and select Device Center.

2 Click Resources > Fonts.

3 Select PS Fonts.

A list of the fonts that currently reside on the Fiery server appears.

4 To add or update fonts, click Add New. Click Add to locate the font that you wish to download, and then click OK and Refresh.

You can add Adobe PostScript Type 1 fonts.

5 To delete a font, select an unlocked font in the Font List and click Delete. Locked fonts cannot be deleted.

6 To print the Font List, click Print.

7 If you added PostScript fonts, re-enable Security > PostScript Security.

Back up and restore fonts

You can back up and restore all fonts on the Fiery server. You cannot select individual fonts.

You must be logged in as Administrator to back up and restore fonts on the Fiery server.

1 Open Device Center in one of the following ways:

- Click the More icon (three vertical dots) next to the server name in the Servers pane.
- Double-click the server name in the Servers pane.

- Click Server > Device Center.
- Right-click the server name and select Device Center.

2 Click Resources > Fonts.

3 Click Backup or Restore.

4 In the web browser window that appears, follow the security prompts.

5 Under Backup Resources and Settings, click Backup Now.

6 Log in as administrator if you are prompted.

7 In the list of items to back up, select Fonts.

8 Observe these guidelines:

Do not back up fonts to an internal drive that also contains the Fiery server. You must restore fonts only to the same Fiery server from which the fonts were originally backed up.

Exit Configure

Some changes won't take effect until you reboot the Fiery server. If a setting change requires a restart, reboot, or other action, the banner at the top of the page will display a message.

1 Make the appropriate changes.

If you are making multiple setting changes that require a reboot, you can wait to reboot until you have finished making all your setting changes.

2 Reboot the Fiery server so that the changes take effect.

View, save, or print server settings

The Server Configuration tab in Command WorkStation lists the current Fiery server settings.

View server configuration settings

From the Server Configuration tab, you can view categories of Fiery server settings or change the Setup options.

1 From Command WorkStation, connect to the desired Fiery server and click Device Center > General > Server Configuration.

2 Do one of the following:

- Click the shortcuts on the left side of the page to view settings for a particular category.
- Click Configure in the bottom-right corner of the window to change current Fiery server Setup options.

Save the server configuration as a file

You can save the server configuration as a file for each Fiery server you are connected to. This is especially useful if you are managing multiple Fiery servers and want to keep track of any changes made in Fiery server Setup.

1. From Command WorkStation, connect to the desired Fiery server.
2. Click Device Center > General > Server Configuration.
3. Click Save As.
4. Specify the file name and location.
5. Select PDF or Text for the file type.
6. Click Save.

Print the server configuration page

After you have performed Setup, print the server configuration to confirm your settings, and post it near the Fiery server for quick reference. Users need the information on this page, such as the current default settings.

1. Save the configuration file.
2. Print the saved file to an office printer.

About backing up and restoring

You can back up either the Fiery Resources and Settings, or an entire system image of the Fiery server.

For more information about backing up the system image, see *Configuration and Setup*, which is part of the user documentation set.

Back up Fiery server settings from Command WorkStation (FS400/400 Pro and later)

From Command WorkStation, you can choose which Fiery server settings you want to back up.

We recommend that you save the backup file to a network server, not the Fiery server itself. Otherwise, when you reinstall system software, the backup file is deleted.

Settings can be restored to another Fiery server of the same model and version, but settings such as Server Name, IP address and Network settings are not restored; the existing settings remain untouched. This prevents problems with both Fiery servers co-existing on the same network.

1. Connect to the Fiery server as Administrator and do one of the following:
   - Click Device Center > General > Tools > Fiery Resources and Settings.
   - Select Server > Backup and Restore.
2. In the new web browser window that appears, click Fiery Resources and Settings.
3. Click Backup Now.

4 Select the items you want to back up and click Continue.

5 In the dialog box that appears, specify a name for the backup file.

6 (Optional) Select Add date to file name.

7 Click Continue.

8 Download the file you want and specify a location for the file.
You must choose an .fbf file and a .DAT file.

Restore Fiery server settings from Command WorkStation (FS400/400 Pro and later)

If you previously backed up Fiery server settings, you can restore them from Command WorkStation.
Settings can be restored to another Fiery server of the same model and version, but settings such as Server Name, IP address and Network settings are not restored; the existing settings remain untouched. This prevents problems with both Fiery servers co-existing on the same network.

1 Connect to the Fiery server as Administrator and do one of the following:

- Click Device Center > General > Tools > Fiery Resources and Settings.
- Select Server > Backup and Restore.

2 In the new web browser window that appears, click Fiery Resources and Settings.

3 Click Restore.

4 In the dialog box that appears, click Choose File and browse to the location of the configuration settings you want to restore and click Open.
You must choose an .fbf file and a .DAT file.

5 Click Continue.

6 Select the items you want to restore and click Continue.

7 After the restore operation is complete, reboot the Fiery server if you are prompted.

Troubleshooting

These troubleshooting steps can help to resolve the most common issues.

For additional information or support, registered users may start a discussion through EFI Communities. You can also see *Fiery Command WorkStation Help*.

1 Confirm that all the cables required for the Fiery server are intact and firmly seated in the correct ports.
The most common cause of an issue is a faulty or loose cable.

DANGER Do not remove the covers or otherwise open the Fiery server hardware. The parts inside the chassis and internal cables are intended to be serviced by authorized service technicians only.

2 If the Fiery server cannot power on, confirm that the power cord is intact and adequate power is available at the power outlet.

3 If the Fiery server is printing slowly or is not managing jobs as expected, review the Fiery server configuration to confirm the settings are optimal for your network and print environment.

Any changes to your network environment or workflow may require changes to the Fiery server configuration.

4 Confirm that third-party applications are not installed on the Fiery server.

Third-party applications are not supported on the Fiery server and can cause system problems. This includes multimedia messaging service (MMS) applications (they can be installed on client computers or on the network).

5 Confirm that any anti-virus application used to scan the Fiery server is set to run upon request only, and is not in continuous operation.

6 Confirm that the operating system settings on the Fiery server are not modified and the operating system is not upgraded (unless approved by technical support).

Changes to the operating system settings or version can cause system problems.

7 Confirm that the Windows firewall has not been disabled.

8 Review any error messages showing in the Command WorkStation Servers list.

9 Take a screenshot of the Command WorkStation display and any error messages, then close and reopen Command WorkStation. If any error messages display when it restarts, contact technical support.

10 You can use the Preflight option to check for errors. For more information, see *Fiery Command WorkStation Help*.

11 Reboot the Fiery server. If the Fiery server does not reach the Idle state or any other issues remain, collect the related information and contact technical support.

Create Job Error Reports

When you create a job error report, Command WorkStation creates a zip file of the current job files, logs, and information about the Fiery server. You can generate a job error report even if the print job is not in an error state.

Note: The error log entries are overwritten after a period of time. To ensure the error logs contain the relevant information, create the job error report as soon as possible after the error is observed. Create the job error report before rebooting the Fiery server and if possible, before any additional print jobs are processed or printed.

You can create a job error report for any jobs in the Held list.

1 In Command WorkStation, select a job in the Held list.

2 If you are accessing from a Windows computer, press Ctrl and right-click the job. If you are accessing from a Mac computer, press Command+Control and right-click the job.

3 In the shortcut menu, click Create Error Report.

4 Enter information about the job error.

a) Enter any comments and additional details in the text field.

We recommend including the following information:

- Date and time error occurred
- Observed error codes, if any
- Description of expected result
- Description of incorrect result

- Steps for how error occurred
- Frequency of error (such as single event, rarely, sometimes, frequently, always)
- Whether the error has occurred with more than one file
- Whether the file selected for the report is the same file that had the error
- Operating system version, if the print job was sent from a client computer
- Version of Fiery server user software installed
- Description of any other actions performed on the Fiery server during the same time period

b) Optional: If the job includes raster data, you can include it in the report by selecting Rasters.

The raster can be useful to include if the file is not processed correctly. However, it may exceed the allowed size of the report. In this case, it may be useful to provide it separately.

c) Optional: If the job includes color profiles in the report, you can include them in the report by selecting Color Profiles.

Color profiles can be useful to include if they are custom profiles and the printed colors are incorrect.

d) Optional: To include the native source file in the report, click Add +.

The native source file can be useful to include if the job does not process or print. However, it may exceed the allowed size of the report. In this case, it may be useful to provide it separately.

5 Attach any additional related files to the report.

The job error report has a maximum file size of 2GB. If the selections and attachments result in a report larger than 2GB, the report must be reduced in order to be completed.

6 Optionally, if any print jobs are considered confidential, remove the job files before sending the zip file to technical support.

To remove the confidential job files from the Job Error Report, follow the steps:

1 Extract the content from the Job Error Report zip file.

2 Open the extracted folder.

3 Delete the confidential job file.

4 Compress the folder and send it to the technical support.

7 Save the job error report.

Download system logs

You can download the system logs from Configure. These logs are saved as a ZIP file to your computer and can be sent to Technical Support for troubleshooting purposes.

1 In Configure, click Fiery Server > System Logs.

2 Click Download.

Resolve runtime errors

Most runtime errors are related to connection issues and can be easily resolved using the tips provided in this section.

Printer not found

Most failures to find a printer on the network are due to a missing or conflicting name or IP address for the Fiery server.

On the Fiery server:

- Make sure that the host name (DNS name) is entered at Configure > Fiery Server > Server Name. For more information, see *Fiery Command WorkStation Help*.

On each Windows or Mac client computer:

- Ping the Fiery server from the client computer, and perform standard troubleshooting of any connection issues.
- If standard troubleshooting does not resolve the issue, then you can specify the Fiery server host name (DNS name) in the hosts file.

  Note: Once you specify the host name on the client computer, it must be updated each time the name changes.
- To allow Command WorkStation and other Command WorkStation utilities on the client computer to connect to the Fiery server, the Fiery server IP address or DNS name must be configured in the server list. For more information, see *Utilities*.

Cannot connect to the Fiery server with Command WorkStation or utilities

If you cannot connect to the Fiery server with Command WorkStation or the utilities, check the network connectivity and verify that the users are entering the correct IP address or DNS name.

- A remote computer running utilities or WebTools may be interfering by obtaining status information. If possible, close the remote application, and try to connect again.
- Restart the Command WorkStation software and try to connect again.
- Reboot the Fiery server.

Verify the configuration settings on the Fiery server. If you cannot connect with Command WorkStation, use WebTools Configure.

- In Configure > Fiery Server, check the setting for Server Name.
- In Configure > Network, check the IP address settings and other network settings.
- On the client computer, confirm that the required network protocols are loaded.