# Security: Remote Development Services (RDS)

Last update: Aug 27, 2026

Remote Development Services (RDS) lets IDE tools connect remotely to a ColdFusion server and requires careful security control.

## Overview

Remote Development Services (RDS) is a ColdFusion feature that allows IDE tools like the VS Code extension to connect remotely to a ColdFusion server. RDS lets you access files and datasources registered in the ColdFusion Administrator, letting developers browse files, run database queries, execute code, and debug against a remote server.

RDS must be enabled as part of your ColdFusion server install (or when installing the VS Code Plugin) before it can be used. While useful during development, RDS provides significant server access and must be carefully controlled. Adobe recommends that you do not use RDS on public-facing or shared hosting machines.

## Disable RDS in ColdFusion Administrator

Adobe recommends disabling RDS on production servers because RDS provides remote access to ColdFusion files and registered data sources.

If ColdFusion was installed using the Production configuration (or with **Enable Secure Profile** in Security settings enabled), RDS is disabled by default during that installation. You don't need to disable it separately. The following steps are for verifying that, or for disabling RDS manually if it was installed with the Development configuration and later needs to be locked down.

To disable RDS:

1. Log in to the ColdFusion Administrator.

2. In the left navigation, select **Security > RDS**.
3. Locate the **Enable RDS Service** setting.
4. Disable the RDS service.
5. Save or submit the changes.
6. Verify that RDS access is no longer available.

> **IMPORTANT**
>
> RDS provides direct file system and database access to your server. It should be disabled on production servers and only enabled on development/staging environments with proper authentication and network restrictions.

## RDS configuration settings

Controls whether RDS is enabled and what authentication is required.

**Enable RDS**

### Purpose

### Default

### Recommendation

### Impact

> **IMPORTANT**
>
> Enabling RDS on production servers exposes your file system, database connections, and server resources to potential unauthorized access. Only enable on isolated development environments.

**RDS password**

### Purpose

**Default** +

**Recommendation** +

**Security** +

## Best practices

- Use a password manager to generate and store a complex password.
- Never use the same password as the ColdFusion Administrator.
- Rotate the password regularly (every 90 days minimum).
- Never share RDS passwords via email or chat.
- Change it immediately if compromise is suspected.

## Enable separate password for RDS and Administrator

**RDS Dataview and Query Viewer (VS Code Extension)**

To use RDS, enable RDS while installing the VS Code Plugin. The extension provides views to access files and datasources on local and remote servers.

- **RDS Dataview** displays the datasources configured on a remote server. When you add a ColdFusion server instance in the extension, it automatically becomes available in the RDS Dataview.
- **RDS Query Viewer** lets you create and run queries against a selected datasource, and is available from the RDS Dataview toolbar.

To create and execute a query using the RDS Query Viewer:

1. Right-click any datasource and select **RDS Query Viewer**.
2. In the *RDSViewer.sql* editor, build a query using any datasource and table.
3. Select **Execute Query**.
4. View the results in the Query Viewer.

# Security best practices

**Production environment: Mandatory security requirements**

- Disable RDS completely. No exceptions for production.
- Verify RDS is disabled in the Administrator before deployment. If ColdFusion was installed with the Production configuration or Secure Profile, this should already be the case, but confirm rather than assume.
- Verify RDS is disabled in the Administrator before deployment (RDS cannot be reliably disabled via firewall rules alone. It shares ColdFusion's own port, so blocking that port blocks all of ColdFusion, not just RDS).
- Optionally restrict ColdFusion's web-server port as a whole at the firewall. This reduces overall exposure but does not substitute for disabling RDS.
- Remove or restrict */CFIDE* directory web access.
- Include an "RDS disabled" check in the deployment checklist.
- Monitor logs for any RDS connection attempts.

> Important: Most security frameworks (PCI-DSS, SOC 2, ISO 27001) require RDS to be disabled on production systems due to the extensive access it provides.

**Development environment: Secure RDS usage guidelines**

- Enable RDS only on local development machines.
- Use strong, unique passwords (16+ characters).
- Enable separate RDS and admin passwords.
- Never expose ColdFusion's web-server port to the internet (this exposes RDS too, since RDS has no separate port).
- Use a VPN for remote RDS access if absolutely required.
- Restrict access by IP address when possible.
- Disable RDS when not actively developing.
- Use HTTPS for all RDS connections.
- Rotate RDS passwords quarterly.

**IMPORTANT**

RDS is not a separate network listener. It rides on whatever HTTP/HTTPS port serves ColdFusion itself. There is no dedicated "RDS port" to isolate at the network layer.

| Deployment | Port |
|---|---|
| HTTP (standalone ColdFusion) | 8500 (Built-in web server, standalone default) |
| HTTPS (if SSL configured) | Built-in web server, SSL configured, 8501 (the built-in default port, not an HTTPS-specific RDS port) |
| JEE Deployment | Uses the web server port (80/443) with the */CFIDE* path |

**Firewall rules:** You can't firewall RDS separately from ColdFusion. Blocking ColdFusion's web-server port blocks the application, the Administrator, and RDS together. There's no port-level control that disables RDS alone. Disabling RDS in the Administrator is the only reliable control; firewall rules should be used to restrict ColdFusion as a whole, not RDS specifically.

**Example: Linux iptables**

```
# Allow RDS HTTP from a trusted IP only
iptables -I INPUT -p tcp -s 192.168.1.100 --dport 8500 -j ACCEPT

# Allow RDS HTTPS from a trusted IP only
iptables -I INPUT -p tcp -s 192.168.1.100 --dport 8501 -j ACCEPT

# Allow from a local subnet (adjust as needed)
iptables -I INPUT -p tcp -s 192.168.1.0/24 --dport 8500 -j ACCEPT
iptables -I INPUT -p tcp -s 192.168.1.0/24 --dport 8501 -j ACCEPT

# Save rules
service iptables save
```

**Example: Windows Firewall (PowerShell)**

```
# Allow RDS HTTP from a specific IP
New-NetFirewallRule -DisplayName "Allow RDS from Dev IP" `
```

```
  -Direction Inbound -LocalPort 8500 -Protocol TCP `
  -Action Allow -RemoteAddress 192.168.1.100

# Allow RDS HTTPS from a specific IP
New-NetFirewallRule -DisplayName "Allow RDS HTTPS from Dev IP" `
  -Direction Inbound -LocalPort 8501 -Protocol TCP `
  -Action Allow -RemoteAddress 192.168.1.100
```

## Verify RDS status programmatically

```
/**
 * Check if RDS is enabled on the server
 * Useful for deployment verification scripts
 * NOTE: let this throw on failure — do not swallow errors into a "false"
 * since that would misreport RDS as disabled when the check itself faile
 */
function isRDSEnabled(required string adminPw) {
    createObject("component", "cfide.adminapi.administrator").login(argum
    return createObject("component", "cfide.adminapi.security").getEnable
}

// Usage in a deployment script
if (isRDSEnabled(adminPassword)) {
    writeLog(file="deployment", type="error", text="SECURITY ALERT: RDS i
    // Fail deployment or send alert
}
```

```
/**
 * Enable or disable RDS programmatically
 */
createObject("component", "cfide.adminapi.administrator").login(adminPass
security = createObject("component", "cfide.adminapi.security");
security.setEnableRDS(false);              // false = disable (productior
security.setUseSingleRDSPassword(false);   // false = keep RDS and Admin
security.setRDSPassword(newRdsPassword);   // set/rotate the RDS passwor

// Related: enableRDSServlet() / disableRDSServlet() control the RDS serv
```

Share this page

Was this page helpful? Yes, thanks Not really

**ColdFusion**
Overview
Features
Pricing
Free Trial
Terms of Use

**Support**
Download and install
Help Center
Adobe Support
Community
Enterprise Support
Genuine software

**Resources**
Adobe Blog
Adobe Developer

**Adobe Account**
Log in to your account

**Adobe**
About
Careers
Newsroom
Corporate responsibility
Investor Relations

**Featured products** AEM Guides Adobe Captivate Adobe Learning Manager Adobe Connect

Copyright © 2026 Adobe. All rights reserved. Privacy / Terms of Use / Cookie preferences / Do not sell my personal information / AdChoices