ACCOUNTING CS

Setup Instructions for Firm-Hosted Client Access

TL 32076 (12/21/18)

Contents

Overview

Because Accounting CS and Accounting CS Client Access share a common database, both are required to run in a hosted environment — **either** through our Thomson Reuters servers using Virtual Office CS® or Software as a Service **or** through your firm's own hosted environment.

To set up the hosted environment on your firm's own servers, first follow the instructions in Accounting CS Installation and Program Essentials (PDF) to install Accounting CS on your firm's terminal server. You will then need to complete additional (one-time) setup steps outlined in this guide that will enable you host Accounting CS Client Access in your firm-hosted environment. Finally, you will need to complete setup steps for each client within Accounting CS, by following the procedures in our Help & How-To Center.

Note: Your **clients'** experience with starting and using Accounting CS Client Access is not affected by your choice of hosting environment — firm-hosted with full SQL Server, Virtual Office CS, or Software as a Service (SAAS).

Important considerations critical to your firm's data security

Because multiple clients will have direct access to a shared database on your firm's terminal server, and to ensure that only authorized personnel can access your firm's critical data and settings, **be certain to rely only on a terminal server professional who is certified and qualified to handle this type of installation.** Our CS Support staff at Thomson Reuters will **not** be able to assist with setting permissions, publishing applications, or making changes to Group Policy Objects (GPO) or user accounts.

For general information to provide to your firm's terminal server technician, please refer to Terminal Server Best Practices for CS Professional Suite Applications (PDF), which is accessible from our Help & How-To Center.

System requirements for Firm-Hosted Client Access

Important! Be sure to review other application requirements as well, which may not be compatible.

Microsoft licensing

- A Microsoft®-supported version of full SQL Server® 2012 (or a newer version) (For performance reasons, MS SQL Server Express is **not** recommended for firm-hosting of Accounting CS Client Access.)

  Note: Support for Microsoft SQL Server 2008 and 2008 R2 will be discontinued in July 2019. For details, see Discontinued support for Microsoft SQL Server 2008 in our Help & How-To Center.

- Microsoft Volume Licensing – Client Access License (CAL)
- Microsoft Terminal Server licensing

CS Professional Suite licensing

- Accounting CS and/or Accounting CS Payroll
- Accounting CS Terminal Server licensing
- Firm-Hosted Client Access licensing (code “ACSFHCA,” which is available free of charge from your CS Sales Representative)
- NetFirm CS® licensing
- NetClient CS® portal for each client user

More details

- Because the software is accessed via the internet and information travels through an internet connection, the performance of the software is subject to the same speed variations experienced using the web. For this reason, the bandwidth used when accessing the internet has a significant impact on the performance of the software. To achieve optimal product performance, we recommend a persistent internet connection with a minimum bandwidth of 128 Kbps for up to four users and 32 Kbps for each additional, concurrent user. Examples of internet connections that meet these recommendations include dual-channel ISDN, cable modem, ADSL or DSL, T1, and T3.
- As with most of our applications, a browser is required. We recommend a minimum of 128-bit encryption.
- For optimal results when printing from any application running in the hosted environment, we recommend that both you and your clients use a native printer for your operating system (Windows Server 2008, 2008 R2, or 2012).

  For a complete list of printers that we recommend for use in Virtual Office CS, see Printer drivers available in Virtual Office CS in our Help & How-To Center.

Verifying the Accounting CS database name

Accounting CS Client Access requires that the Accounting CS database name use the following format:

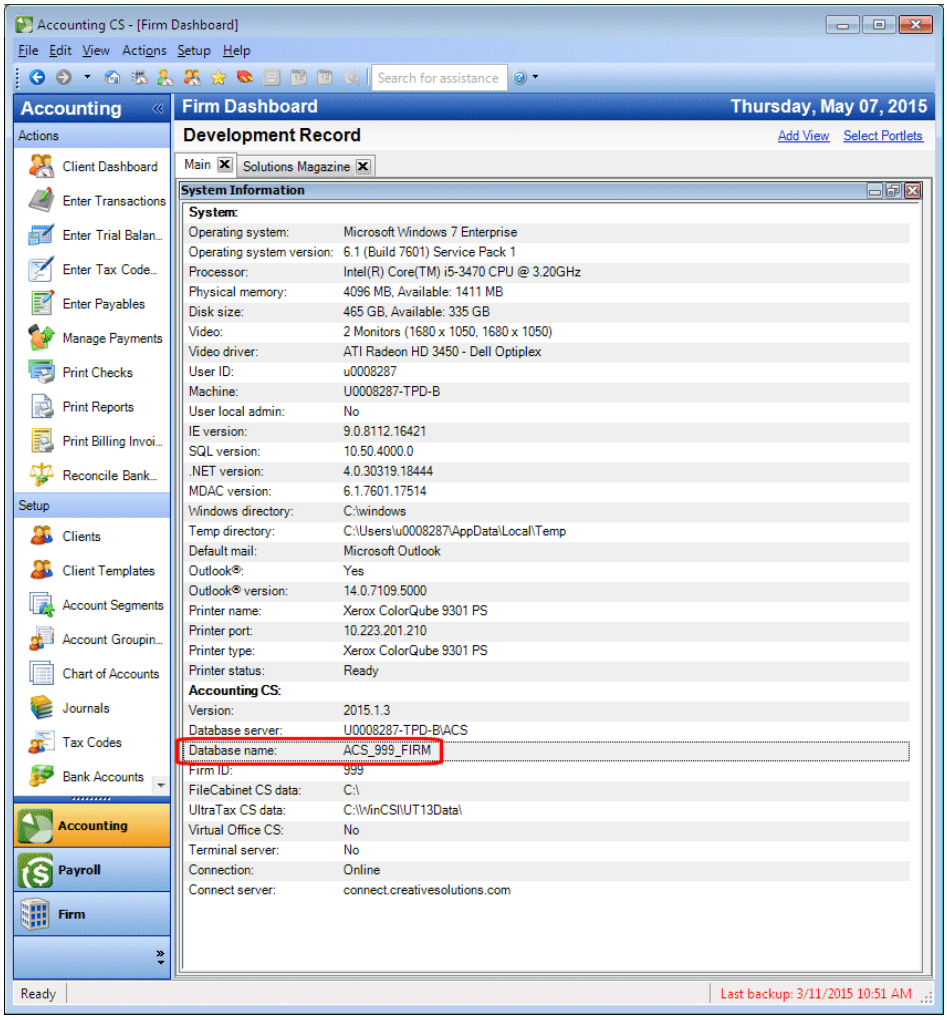
ACS_<firm ID>_FIRM, where <your firm ID> represents your firm's ID.

For example, if your firm ID is 999, then your Accounting CS database must be named **ACS_999_FIRM**.

Follow these steps to verify the database name.

1. Add the Systems Information portlet to any of your Dashboards.
    a. In the Home, Firm, Staff, Client, or Workpapers Dashboard, click the view for which you want to add the System Information portlet.
    b. Click the *Select Portlets* link in the upper-right corner of the screen.
    c. In the Select Portlets dialog, mark the *System Information* checkbox and click OK.
    d. Position the portlet in the desired location in the view.

2. In the Accounting CS section of the System Information portlet, check the name in the **Database name** field.



3. If the database name does not conform to the required format, have your qualified IT technician verify the name of the Accounting CS database in SQL Management Studio.

Note: For information on renaming SQL databases, see https://msdn.microsoft.com/en-us/library/ms345378.aspx on the Microsoft website.

One-Time Terminal Server Setup Steps

Accounting CS Client Access is installed on your firm's terminal server at the same time that you install Accounting CS. To properly configure Accounting CS Client Access, you will need to complete the following setup steps **after** installing Accounting CS.

These setup steps should be done from the terminal server console by a qualified technician with Domain Administrator access rights.

Configure the shared files

1. Navigate to the folder on the terminal server where the Accounting CS shared files are installed (default location is X:\WINCSI).
2. In the X:\WINCSI folder, create a new folder called **Accounting CS Client Data**.
3. Copy the following from the X:\WINCSI\Accounting CS Data folder to the new X:\WINCSI\Accounting CS Client Data folder:
   - Datasource.xml (file)
   - The complete folder structure (folders only without files)

Configure the LocalInstallation.ini file

1. On the terminal server, navigate to the C:\ProgramData\Creative Solutions folder and create a new subfolder called **Accounting CS Client**.

   Note: The ProgramData folder is typically a hidden folder, by default. If have difficulty locating this folder, ask your system administrator for assistance .

2. Within the Accounting CS Client folder, create a blank text file named **LocalInstallation.ini**.

3. Open the LocalInstallation.ini file in Notepad and then copy the text below and paste it into the LocalInstallation.ini file:

   [appSettings]
   ; location of the Accounting CS shared files area. Default value below
   NetworkInstallationFolder=X:\WinCSI\Accounting CS\

   ; location of the Accounting CS program. Default value below
   LocalInstallationFolder=X:\Program Files (x86)\Creative Solutions\Accounting CS\

   ; location of shared application data. You must set up this location manually after installing the Accounting CS application. Default value below
   AppDataPath=X:\WinCSI\Accounting CS Client Data\

4. After pasting the information listed into the LocalInstallation.ini file, change the X: \WinCSI\<folder path> to the drive location where the WinCSI folder exists for your firm.

Verify Windows security settings

Windows Security should be used to prevent client users from accessing sensitive information on your firm's servers.

Each client user will need the following general security rights to access folders on your terminal server:

- Read/execute access to the application's runtime folder in **\Program Files (x86)\Creative Solutions\Accounting CS**.
- Read access to the **WINCSI\Accounting CS** folder.
- Read/write to the **WINCSI\Accounting CS Client Data** folder.
- Read access to the **WINCSI\Licenses** folder.

We strongly recommend that you publish the application rather than provide a desktop to clients. However, if you must provide a desktop, we recommend using mandatory profiles with appropriate restrictions **to limit access** to the following:

- Control Panel
- Other applications
- Right-clicks
- Rebooting the server

One-Time Steps to Configure Accounting CS for Use with Client Access

This chapter covers the one-time setup steps you need to complete before setting up your first business client to use Accounting CS Client Access within your firm's hosted environment.

Setup procedures

Before you can set up or save any changes within Accounting CS for the staff of any business client, you must first create a Remote Desktop Protocol (RDP) file and then select that file from the Firm-Hosted Client Access section of the Firm screen in Accounting CS.

1. Create an RDP file that points to the **AccountingCSClient.exe** file on the server where Accounting CS Client Access is installed and save a copy of that file locally.

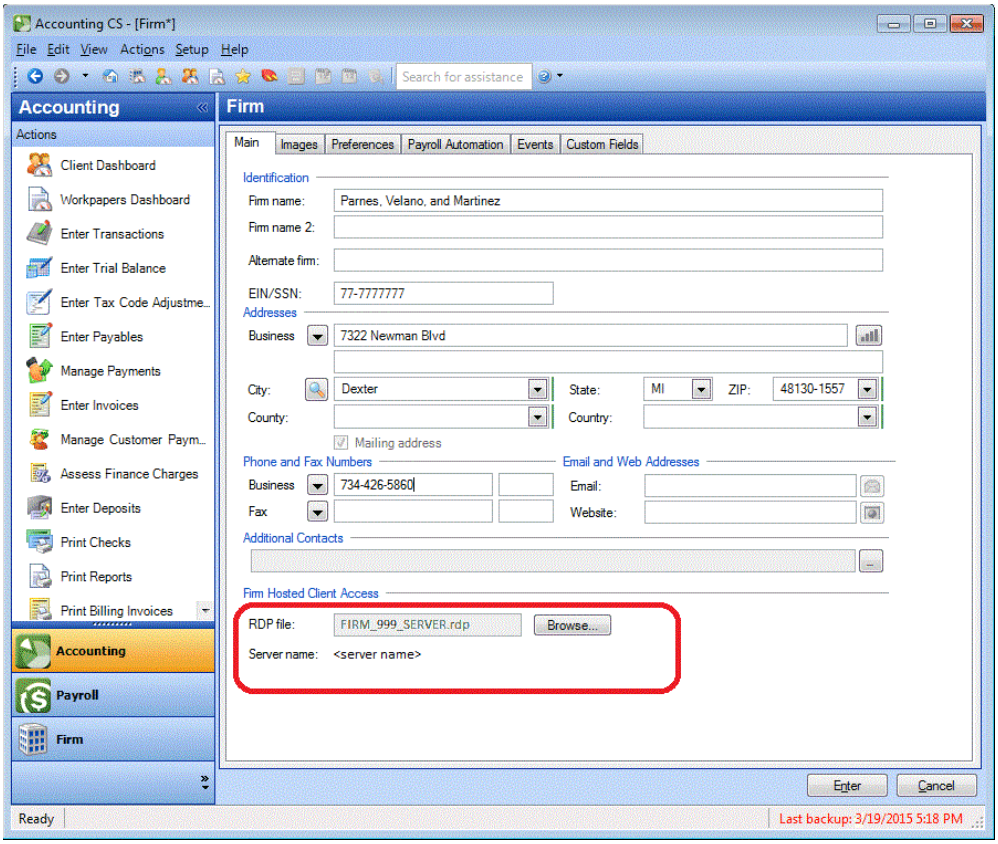
   To create an RDP file that launches only Accounting CS Client Access and not a full desktop, you need to add it as a listed Terminal Server program.

   Note: If you receive an "access denied" message when launching from the RDP file, please do the following: (a) Open Server Manager and choose Roles > Terminal Services; (b) right-click RemoteApps, choose Terminal Server Settings > Access to Unlisted Programs, and change that setting to **Allow users to start both listed and unlisted applications**.

2. Start Accounting CS and choose Setup > Firm Information > Firm.

3. In the Firm-Hosted Client Access section of the Main tab, click the Browse button and then navigate to and select the RDP file that you created in step 1 above. (See the illustration on the following page.)

4. Press ENTER to save your changes and upload the RDP file to NetClient CS.



Enabling firm security

Before you can enable Accounting CS Client Access services for any client, you must first enable firm security features for your own firm within Accounting CS.

1. Choose Setup > Firm Information > Firm and click the Preferences tab.
2. Mark the *Enable firm security* checkbox. This setting also enables anyone with Administrator privileges to specify security settings for staff groups, including their ability to access selected areas of the application.
3. Press ENTER to save your changes. You will need to restart the application for the security changes to take effect.

Steps for Client Setup

This chapter highlights the specific setup steps you need to complete for clients to enable them to use Accounting CS Client Access.

Note: For details, see Client setup, overview and Setting up a client for Accounting CS Client Access in our Help & How-To Center.

Setting up a client for Accounting CS Client Access

1. In Accounting CS, choose Setup > Clients.
2. **For new clients in Accounting CS:**
   Click the Add button and, in the Add Client dialog, enter or select the appropriate information in the Identification, Address, and Services sections. Also mark the *Enable Client Access* checkbox, make the appropriate selections in the Client Access Services sections, and then click the Add button. Enter additional information in the Clients screen as necessary.

   For existing clients in Accounting CS:
   Select the client and click the Edit button. Click the  button in the Services section of the Main tab in the Clients screen, mark the appropriate checkboxes and options in the Add/Remove Services dialog (including the *Enable Client Access* checkbox), and then click OK. Add or update additional information in the Clients screen as necessary.
3. Click the Enter button to save the client information.
4. Follow the steps (below) to set up client security groups.
5. Follow the steps (below) to set up client staff.

Note: The features and menu commands that will be available for the client to see and access in Accounting CS Client Access depend on the services and security options that you select for the client staff members who will be using the application.

Set up a client security groups

Create a security group for each set of application features (or client staff roles and responsibilities) that you want client staff to be able to access.

1. Choose Setup > Firm Information > Client Security Groups and click the Add button.
2. Enter a name for the new security group in the *Description* field.
3. In each tabbed page in the Security Group Information section, mark the checkbox next to the permissions you want to assign to the client security group.
4. Click the Enter button.

Set up client staff

After you enable the Client Access service for a client and set up appropriate client security groups, you can enter information for the client staff members who will work in Accounting CS Client Access.

1. Choose Setup > Firm Information > Client Staff.
2. In the Main tab of the Client Staff screen, enter basic identification and contact information for each staff member. At a minimum, you must enter information in the *ID* field to be able to save the record and in the *Last* (name) and *Email* fields to initialize the individual's NetClient CS portal.
3. If the individual already has a NetClient CS account, click the  button in the NetClient CS Access section. In the NetClient User Account dialog, mark the checkbox for the NetClient CS account to assign to this client staff member.
4. Click the Security tab, and then mark the checkboxes for all security groups that apply to the individual's role within the client's business.
5. Click the Client Access tab. In the Selections grid, mark the checkbox in the Allow column for each client ID to which this client staff member should have access. The grid includes all clients for which one or more of the Client Access Services checkboxes are currently marked in the Add Client dialog or the Add/Remove Services dialog.
6. Click Enter to save the information.

Important! You must select an RDP file in the Firm-Hosted Client Access section of the Main tab of the Setup > Firm Information > Firm screen before you can set up or save any changes for client staff.

Resetting passwords

If a client staff member loses or forgets his or her Accounting CS Client Access login password, the firm administrator (or a firm staff member with privileges for the Security tab of the Client Staff setup screen) can reset the password.

1. Choose Setup > Firm Information > Client Staff.
2. In the Client Staff screen, click the Security tab.
3. Highlight the staff ID and click Edit.

4. Click the Reset Password button.
5. Click Yes to confirm the action.

The next time the client staff member opens the application, he or she will be prompted to enter a new password.

Activating a NetClient CS portal

Note that this procedure is to be completed by the client.

When you save a client staff record in Accounting CS, NetClient CS sends an email message to that individual (if there is no existing account data for the client and if a valid email address is provided for the client staff member). The email message provides a link that the individual must click to activate their portal. Once the account has been activated, the client staff member can begin using the features in Accounting CS Client Access (as determined by their specific security settings.

Note: If you need to resend the account activation email message to a client (for example, if the client staff member accidentally deleted the original message), you can click the Resend Registration Email button in the Main tab of the Client Staff screen. This prompts NetClient CS to resend the email message to the client.

Additional Details and Special Procedures

Direct Deposit processing

The following notes are important to keep in mind if your firm processes direct deposit files for a client who is set up to use Accounting CS via their NetClient CS portal.

- Because your firm and your clients who use Accounting CS Client Access share the same firm database, you share the same bank account direct deposit setup information. Your firm enters and controls the information in the Direct Deposit tab of the Setup > Bank Accounts screen or the Setup > Firm Information > Impound Bank Accounts screen. This tabbed page is not available to your clients.
- If both your firm and your client send ACH files to the same bank, the direct deposit information for that bank is shared. If your client needs to send ACH files to the same bank using a different direct deposit setup, they can use the Client Direct Deposit tab of the Setup > Bank Accounts screen to set up a second bank account record to define their own direct deposit settings for the bank. This may be necessary if your firm and your client require different details in the 5 Record of the ACH files.

Changing the client's posting period

If you enabled the accounting services for your client, and the client's staff members have security rights to change the posting period, they can move the posting period forward or backward (within the same fiscal year) by choosing Actions > Change Posting Period.

Deactivating Accounting CS Client Access for a client

You can disable Accounting CS Client Access for a client at any time.

There are two components to the process for deactivating Accounting CS Client Access so that no further fees are incurred: one component requires changes in Services section of the Clients screen, and the other requires changes to the portal setup in the Setup > Firm Information > Client Staff screen.

As soon as you disable the client-level component, any client staff member who worked in Accounting CS will no longer have access to the client data in Accounting CS.

Deactivating client-level access to Accounting CS and associated fees

1. Choose Setup > Clients.
2. Select the client for which you want to disable Accounting CS Client Access, and then click the Edit button.
3. In the Main tab, click the  button next to the *Services* field.
4. In the Add/Remove Services dialog, clear the *Enable Client Access* checkbox, and then click OK.
5. In the Clients screen, click Enter to save the client record.

Deactivating the client-staff component and associated fees

Note that you can (a) delete the client staff record, or (b) keep the client staff record but remove access to Accounting CS Client Access. Neither of these actions will delete the NetClient CS user.

To delete a client staff

1. In Accounting CS, choose Setup > Firm Information > Client Staff.
2. Highlight the name of the client staff and click the Delete button.

See also: Changing the status of a client staff member to Inactive

To remove access to Accounting CS for client staff

1. In Accounting CS, choose Setup > Firm Information > Client Staff.
2. Highlight the name of the client staff and click the Edit button.
3. In the NetClient CS Access section of the Main tab, click the Ellipsis  button for the *Account* field.

4. In the NetClient User Account dialog, locate the name of the NetClient CS user, clear the checkbox for that individual, and then click OK.
5. Click the Enter button to save your changes.

See also: Deleting a client portal or a staff portal

Appendix: Examples of Steps to Safeguard Security for Your Firm's Terminal Server

As noted in the introduction to this guide, because multiple clients will have direct access to a shared database on your firm's terminal server and to ensure that only authorized personnel can access your firm's critical data and settings, **be certain to rely only on a terminal server professional who is certified and qualified to handle this type of installation. Thomson Reuters Support staff will not be able to assist with setting permissions, publishing applications, Group Policy changes, or user accounts.**

For general information to provide to your firm's terminal server technician, please refer to Terminal Server Best Practices for CS Professional Suite Applications (PDF), which is accessible from our Help & How-To Center.

Specific considerations for your own firm might be similar to (but not limited to) the following **examples**.

General setup and troubleshooting

- Create an Active Directory domain and give remote access to the terminal server without giving users Domain/Local admin access.
- Ensure that port TCP 3389 is open both on the firm firewall and the client firewall.
- If the *Auto update failed* error message appears when launching Accounting CS Client Access, try using UNC paths in the LocalInstallation.ini file rather than mapped drives.
- Create and update mandatory/roaming profiles.
  (Because users would have desktop access, we recommend setting up mandatory profiles to ensure a consistent user experience and to limit the level of access to the terminal server.)
- Troubleshoot and perhaps install non-native print drivers to avoid issues users might experience when printing under Remote Desktop Protocol.

- Troubleshoot RDP access from various client locations.
  - You must use your external IP address when configuring the RDP file.
  - In the Program tab, click the *Start the following program on connection* option and enter the correct path information for the application when configuring the RDP file to launch the application automatically on connection to the terminal server.
  - Depending on your terminal server configuration, you may also need to do the following to start the application on connection: Choose Server Manager > Roles >Terminal Services > TS RemoteApp Manager > Terminal Server Settings. In the *Access to unlisted programs* section, click the *Allow users to start both listed and unlisted applications* option.
- Test and troubleshoot issues users might experience when sending email from Accounting CS Client Access in a multi-user environment.
- Set an idle connection limit or monitor connections to the terminal server to ensure that users are logged in only when they are working.

Group Policy Object (GPO) restrictions

- FirmGPO (for settings imported through the mandatory profile to speed up logons).
  - Block access to the Control Panel.
  - Block access to printer setup.
  - Hide all Desktop settings and prevent changes to the Desktop from being saved at logoff.
  - Block access to New Connection Wizard and to viewing status of active connections.
  - Block changes to Taskbars and Start Menu settings.
  - Block access to context menus (right-click).
  - Block access to the shutdown command.
  - Block access to Task Scheduler.
  - Block access to Network Connections and My Network Places.
  - Block access to Windows Update.
  - Block access to Run command from the Start Menu.

Restrict user access to specify drive locations

C drive permissions (locations where files can be saved)

Example: Hide C drive from browsing.

- C:\
- C:\$RECYCLE.BIN
- C:\ProgramData
- C:\Users (profiles are not cached and deleted at logoff per MetaFrameGPO)
- C:\Windows\Temp
- C:\Windows\System32\spool\printers

C drive permissions (locations where files cannot be saved)

Users would continue to have Read/Execute permissions to access these locations.

- C:\Boot
- C:\Inetpub
- C:\MSOCache
- C:\PerfLogs
- C:\Program Files
- C:\Program Files (x86)
- C:\System Volume Information
- C:\Wincsi
- C:\Wincsi.net
- C:\Windows

Other drive permissions

Be certain to secure other drives and folders as appropriate for your environment.