



SPIRIT Project

OPERATIONS MANUAL

June 10, 2008_revised_v2

SPIRIT OPERATIONS MANUAL

TABLE OF CONTENTS

1.0	GENERAL INFORMATION	3
1.1	System Overview	3
1.2	Project References	3
1.3	Points of Contact	3
2.0	SYSTEM OPERATIONS OVERVIEW	4
2.1	System Operations.....	4
2.2	Hardware Inventory.....	5
2.3	Software and Operating System Inventory.....	6
2.4	Operational Inventory	7
2.5	Processing Overview	9
2.6	Communications Overview.....	9
2.7	Account Creation.....	10
2.8	Instructions for Updating Vendor Letters	16
2.9	Maintenance and Backup	20
2.10	System Recovery	22
2.11	Environment and Security.....	29
3.0	SITE OPERATIONS OVERVIEW	36
3.1	System Requirements.....	36
3.2	Communication Requirements.....	36
3.3	Troubleshooting FAQ	37
APPENDIX A	40	
Installation Instructions.....	40	
APPENDIX B	62	
Disaster Recovery Plan	62	
APPENDIX C	66	
Glossary of Terms.....	66	
APPENDIX D	75	
End of Month (System Administration).....	75	
APPENDIX E	86	
End of Day (System Administration).....	86	
APPENDIX F	102	
On-going Maintenance, Repair and Replacement of SPIRIT agency equipment	102	
APPENDIX G	103	
Setup Procedures for Data Sync.....	103	

1.0 GENERAL INFORMATION

1.1 System Overview

SPIRIT is an automation system for the Supplemental Nutrition Program for Women, Infants, and Children (WIC Program). This is an on-line, web-based system with a central host that will support clinic and state office functions. The SPIRIT application will automate a number of functions at both the local service delivery sites and the state offices of each SPIRIT Nation WIC Program.

1.2 Project References

All documented processes and design layouts were produced by Covansys.

1.3 Points of Contact

1.3.1 Coordination

A list of organizations that require coordination between the project and its specific support functions, e.g., installation coordination and security will be provided by Chickasaw Nation Information Technology. A schedule for coordination activities will also be included.

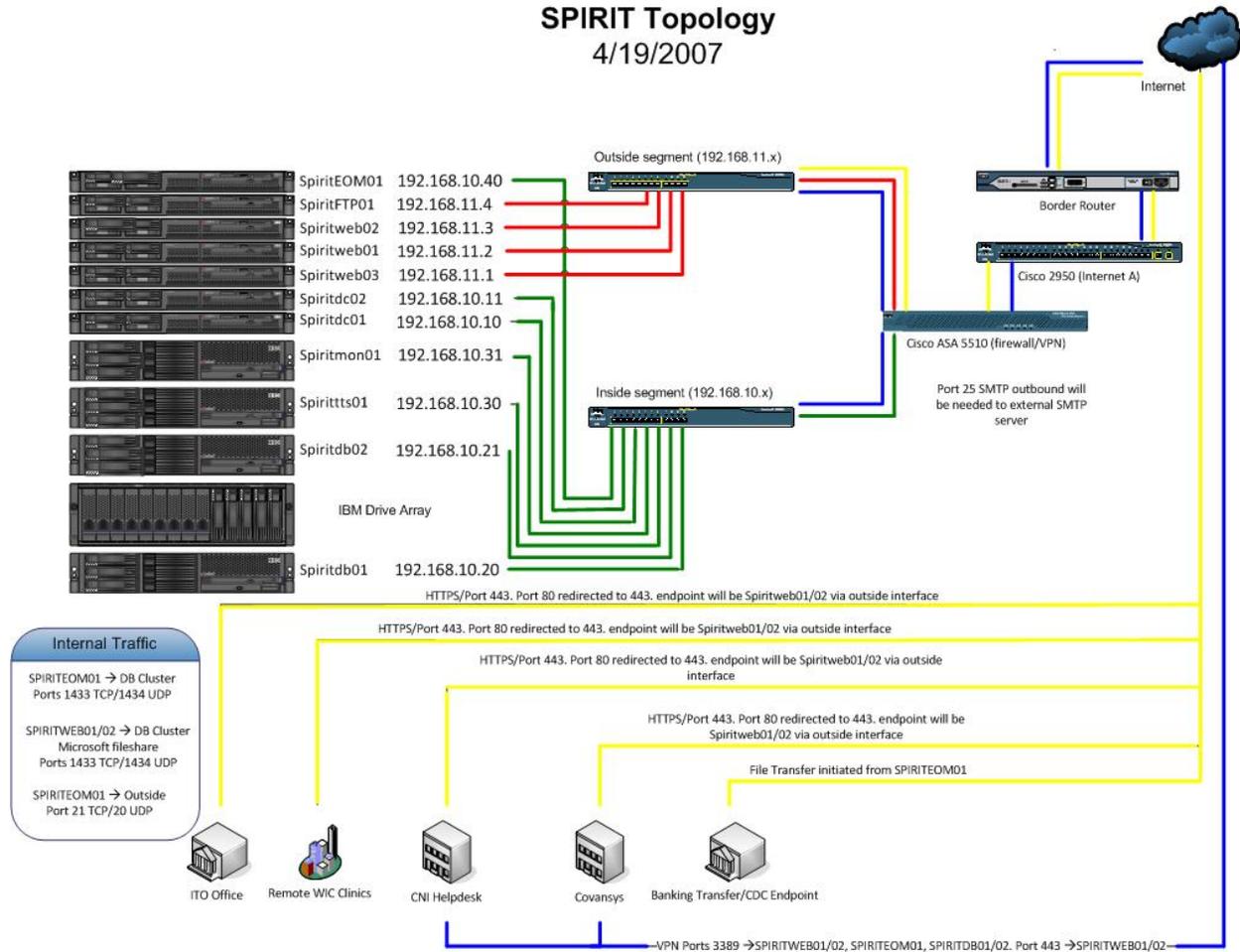
1.3.2 Help Desk

Helpdesk information, including responsible personnel phone numbers for emergency assistance, will be provided by Chickasaw Nation Information Technology.

2.0 SYSTEM OPERATIONS OVERVIEW

2.1 System Operations

SPIRIT is client side web based application.



2.2 Hardware Inventory

Item/Details	Quantity
IBM Server and Storage	
IBM XSeries 336 part# 8837D1U	7
IBM Dual Core Processor part#25R8936	7
HP DL360G4 Intel Xeon 3.6GHz/800 1 MB KitIBM 2GB RAM Upgrade part#73P2866	3
IBM 73GB Hot Swap HD part#40K1023	14
IBM 24X7X4 Hour Response 3yr Remote TS	16
IBM 4GB PC2-3200 part#39M5815	2
IBM 2GB PC2-3200 part#73P4792	4
IBM XSeries 346 2.8GB part#8840D1U	4
IBM Dual Core Processor part#25R8930	2
IBM Server RAID-7KROHS part#39R8800	4
IBM Total STRG FC2-133 HOSTBUS Adptr part#24P0960	2
IBM 1.46GB 10K U320 HS SCSI part#30R5095	10
IBM EXP 400 Storage Enclosure part#17331RU	1
IBM SCSI Bus Expander part#59P5018	1
IBM Hard Drive /73.4 15K part#40K1027	11
IBM Hard Drive 73.4 GB part#53402C	11
IBM ServeRAID 6M Storage Controller part#39R8816	2
IBM Memory 4GB (2x2GB) part#39M5815	3
IBM Remote Supervisor AdapterII part#39M4948	1
Service Pack 24x7x4 part#21P2078	2
IBM Configuration for 11 Servers	1
IBM Processor Upgrade part# 40K2502	2
IBM Service Pak Server part# 21P2078	2
Operating System for DNS Servers	
Solaris 9 1-2 CPU RTU License for Intel Platform	2
Solaris 9 for Intel, Multilingual Media	1
Backup Software and Tapes	
Symantec Backup Exec 11d for Windows Server	1
Symantec Backup Exec 11d Remote Agent for Windows Servers	10
IBM TS3100 Tape Library	1
IBM Ultra320 SCSI Controller 2	1
346xSeries 625W Hot Swap Redundant Power Supply	4
Ultrium 3 Data Cartridges 5-pack	10
336 xSeries 585W Hot Swap Redundant Power Supply	7
Brightstore R.11 UNIX Agent 2 yr maint	2
Firewall Bundle	
PIX 525-FO-GE Bundle (Chassis, Failover SW,2 GE+2 FE,VAC+)	1
Power Cord,110V	1

PIX 525/535 3DES/AES VPN/SSH/SSL encryption license	1
PIX v6.3 Software for the 515E, 525 and 535 Chassis	1
PIX 66-MHz DES/3DES/AES VPN Accelerator Card+ (VAC+)	1
Cisco VPN Client Software (Windows, Linux, Solaris)	1
PIX 66-MHz Gigabit Ethernet int. card, Multimode (SX) SC	1
PIX 66-MHz Gigabit Ethernet int. card, Multimode (SX) SC	1
PIX 525 Failover (FO) feature license	1
SMARTNET 8X5XNBD Chassis ,Failover SW 2GE+2 FE prts, VAC	1
PIX 525-UR-GE Bundle (Chassis, Unrestr. SW,2 GE+2 FE,VAC+)	1
Power Cord,110V	1
PIX 525/535 3DES/AES VPN/SSH/SSL encryption license	1
PIX v6.3 Software for the 515E, 525 and 535 Chassis	1
PIX 66-MHz DES/3DES/AES VPN Accelerator Card+ (VAC+)	1
Cisco VPN Client Software (Windows, Linux, Solaris)	1
PIX 66-MHz Gigabit Ethernet int. card, Multimode (SX) SC	1
PIX 66-MHz Gigabit Ethernet int. card, Multimode (SX) SC	1
PIX 525 Unrestricted (UR) feature license	1
SMARTNET 8X5XNBD Chassis, Unrestr SW, 2GE+2 FE prt, VAC	1
<u>Network Switches</u>	
24 10/100 ports w/2 1000BASE-SX ports, Standard Image only	2
Power Cord,110V	2
8x5xNBD Svc, 24 10/100 ports w/2 1000BASE-SX ports, S	2
1000BASE-SX Short Wavelength GBIC (Multimode only)	4

2.3 Software and Operating System Inventory

2.3.1 Client Desktop Workstations

- HP Compaq Business Desktop dc7700 – PD 945 3.4, part #EN325UT#ABA
- Intel Pentium D processor (Qty 1); 1 GB RAM
- 80 GB hard drive; CD-RW/DVD; 10/100/1000 Ethernet
- Microsoft Windows XP Professional (3 year warranty)
- Microsoft Office Professional and Adobe Reader

2.3.2 Client Laptop Workstations

- Lenovo ThinkPad T60 6369 – Core 2 Duo T7200 2 GHz Centrino Duo
- 1 GB HD
- 1 GB Additional Memory
- 80 GB – CD-RW/DVD
- Windows XP Professional
- Microsoft Office Professional
- Adobe Reader
- SQL Server Enterprise Edition

2.3.3 Laptop Server

- 1400MHz CPU

- 768 MB RAM
- 30GB hard drive
- 56k modem
- Windows 2000
- Microsoft SQL Server

2.4 Operational Inventory

Firewall Bundle	
PIX 525-FO-GE Bundle (Chassis, Failover SW,2 GE+2 FE,VAC+)	1
Power Cord,110V	1
PIX 525/535 3DES/AES VPN/SSH/SSL encryption license	1
PIX v6.3 Software for the 515E, 525 and 535 Chassis	1
PIX 66-MHz DES/3DES/AES VPN Accelerator Card+ (VAC+)	1
Cisco VPN Client Software (Windows, Linux, Solaris)	1
PIX 66-MHz Gigabit Ethernet int. card, Multimode (SX) SC	1
PIX 66-MHz Gigabit Ethernet int. card, Multimode (SX) SC	1
PIX 525 Failover (FO) feature license	1
SMARTNET 8X5XNBD Chassis, Failover SW 2GE+2 FE prts, VAC	1
PIX 525-UR-GE Bundle (Chassis, Unrestr. SW,2 GE+2 FE,VAC+)	1
Power Cord,110V	1
PIX 525/535 3DES/AES VPN/SSH/SSL encryption license	1
PIX v6.3 Software for the 515E, 525 and 535 Chassis	1
PIX 66-MHz DES/3DES/AES VPN Accelerator Card+ (VAC+)	1
Cisco VPN Client Software (Windows, Linux, Solaris)	1
PIX 66-MHz Gigabit Ethernet int. card, Multimode (SX) SC	1
PIX 66-MHz Gigabit Ethernet int. card, Multimode (SX) SC	1
PIX 525 Unrestricted (UR) feature license	1
SMARTNET 8X5XNBD Chassis, Unrestricted SW, 2GE+2 FE prt, VAC	1
Network Switches	
24 10/100 ports w/2 1000BASE-SX ports, Standard Image only	2

Power Cord,110V	2
8x5xNBD Svc, 24 10/100 ports w/2 1000BASE-SX ports, S	2
1000BASE-SX Short Wavelength GBIC (Multimode only)	4

2.5 Processing Overview

2.5.1 Server Overview

#1, #2) Active Directory Server: Primary and Backup Domain Controller

#3, #4) MS-SQL Cluster Server: Application Server Cluster

#5) Application Server – (EOD/EOM)

#6, #7) Web Cluster DMZ

2.6 Communications Overview

Web and database server

Web servers communicate with the MS SQL server on TCP port 1433. The firewall will need to allow the web servers in the DMZ to connect to the database servers on the internal network on TCP port 1433.

Application Server (EOD/EOM) and database servers

Batch processing on this server will connect to the database servers on TCP port 1433.

Communication between Web Servers and Remote Systems:

Permanent connected remote locations

All communication between the user's workstation and the web servers will use Web Services over TCP port 443 (https, SSL).

Non Permanent connected remote locations

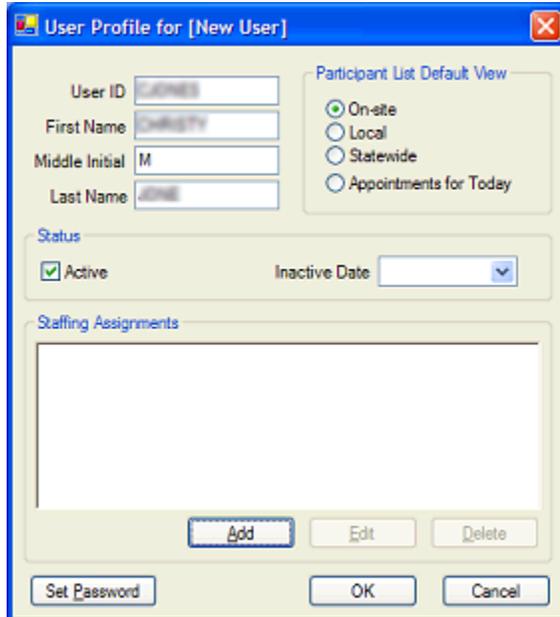
All communication between the user's workstation and the web servers will use Web Services over TCP port 443 (https, SSL). Data replication will transfer data using Web Services over TCP 443.

2.7 Account Creation

The following is a step by step guide for user account creation within the SPIRIT application

2.7.1 Users

The **User Profile** screen is used to manage a user profile record and can be displayed in Add or View mode.



User Profile Screen

To access this screen: Display the **WIC Management Console** screen in Security (Users) mode, and then do one of the following:

- To add a new user profile: On the **Users** menu, click **Add**.
- To view the details of a user profile: Select a user profile in the table > On the **Users** menu, click **View**.

2.7.2 Screen Elements:

User ID – Enter the staff member's user identification.

First Name – Enter the staff member's first name.

Last Name – Enter the staff member's last name.

Middle Initial – Enter the staff member's middle initial.

Participant List Default View – Select one of the radio buttons to indicate which view of the **Participant List** screen to display by default whenever the staff member first launches the application.

Active – Select this check box to indicate the staff member is currently active and able to access the application.

Inactive Date – Enter or select the date on which the staff member's user profile becomes inactive.

Staffing Assignments – View the current staffing assignments for the staff member in the table.

The following buttons are associated with the table:

- **Add** – Click this button to add an assignment to the **Staffing Assignments** table.
- **Edit** – Click this button to edit an assignment selected in the **Staffing Assignments** table.
- **Delete** – Click this button to delete an assignment selected in the **Staffing Assignments** table.

Set Password – Click this button to set the staff member's password.

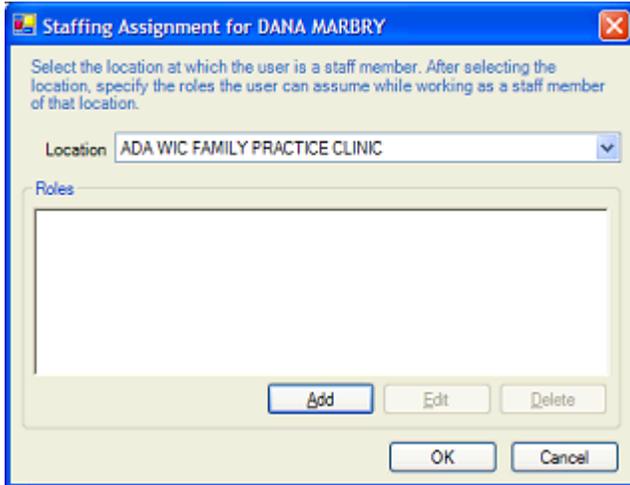
OK – Click this button to process the screen.

Cancel – Click this button to dismiss the screen without processing it.

2.7.4 Assignments, Passwords, and Roles

Staffing Assignment

The **Staffing Assignment** screen is used to manage the staffing assignments for a user profile record and can be displayed in Add or Edit mode.



Staffing Assignment Screen

To access this screen: Display the **User Profile** screen, and then do one of the following:

- To add a new staffing assignment: Click **Add**.
- To edit a staffing assignment: Select an assignment in the **Staffing Assignments** table > Click **Edit**.

2.7.5 Screen Elements:

Location – Select the location at which the staff member has an assignment.

Roles – View the current roles assigned for the staff member in the table. The following buttons are associated with the table:

- **Add** – Click this button to add a role to the **Roles** table.
- **Edit** – Click this button to edit a role selected in the **Roles** table.
- **Delete** – Click this button to delete a role selected in the **Roles** table.

OK – Click this button to process the screen.

Cancel – Click this button to dismiss the screen without processing it.

2.7.6 Set Password

The **Set Password** screen is used to manage password information.

A screenshot of a Windows-style dialog box titled "Set Password for JIM TAYLOR". The dialog box has a blue title bar with a close button (X) in the top right corner. The main area is light gray and contains three text input fields stacked vertically. The first field is labeled "Current Password", the second "New Password", and the third "Confirm New Password". At the bottom of the dialog box, there are two buttons: "OK" and "Cancel".

Set Password Screen

To access this screen: Display the **User Profile** screen > Click **Set Password**.

2.7.7 Screen Elements:

Current Password – Enter the current password.

New Password – Enter the new password.

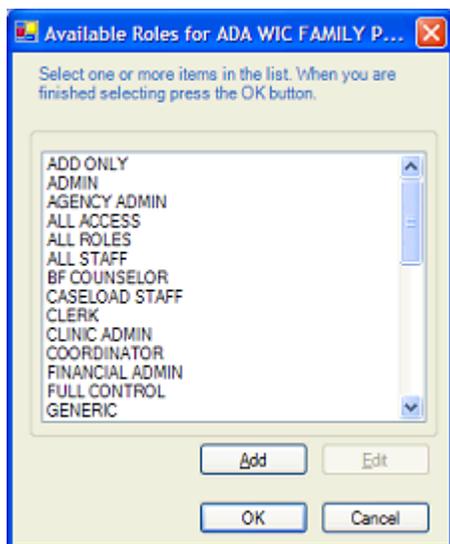
Confirm New Password – Enter the new password again for verification purposes.

OK – Click this button to process the screen.

Cancel – Click this button to dismiss the screen without processing it.

Select Roles

The **Select Roles** screen is used to select a specific role when creating a new staffing assignment.



Select Roles Screen

To access this screen:

Display the **Staffing Assignment** screen > Click **Add**.

2.7.8 Screen Elements:

Available Roles – Select a specific role to assign. The following buttons are associated with the table:

- **Add** – Click this button to add a role to the **Available Roles** table.
- **Edit** – Click this button to edit a role selected in the **Available Roles** table.

OK – Click this button to process the screen.

Cancel – Click this button to dismiss the screen without processing it.

2.7.9 Roles

The **Role Profile** screen is used to manage a role record and can be displayed in Add or View mode.

Feature Group	Feature	Access Level
Financial Management	Accounting Schedule	None
Financial Management	Financial Account Inqui	None
Financial Management	Financial Accounts	None
Financial Management	Financial Management	None
Financial Management	Financial Reports	None
Financial Management	Financial Statements	None

Role Profile Screen

To access this screen:

- To add a new role: Display the **WIC Management Console** screen in Security (Roles) mode > On the **Roles** menu, click **Add**.
- To view the details of a role: Display the **WIC Management Console** screen in Security (Roles) mode > Select a role in the table > On the **Roles** menu, click **View**.
- To add a new role while working with a user profile: Display the **Select Roles** screen > Click **Add**.
- To edit a role while working with a user profile: Display the **Select Roles** screen > Select the role to edit > Click **Edit**.

2.7.10 Screen Elements:

Role Name – Enter the name of the role.

Description – Enter a brief description of the role.

Permissions – A list of all available permissions are displayed in the table. Select the **Access Level** per permission by clicking directly in the column. The following button is associated with the table:

- **Reset** – Click this button to reset the list of permissions currently displayed in the **Permissions** table to their initial settings.

OK – Click this button to process the screen.

Cancel – Click this button to dismiss the screen without processing it.

2.8 Instructions for Updating Vendor Letters

Please Note: Text in the letter template that is in << >> brackets are the mail merge value(s) and can never be deleted or modified without program changes. Modifying these fields will cause errors in the Mail Merge process.

Microsoft Word is required to update the Vendor Letters.

Vendor Letters are stored in the **c:\Program Files\Covansys Inc. - BPDS\WIC\Templates** directory.

Before you begin working, copy all letters to a different working directory on your hard drive for modifying. When modifications are completed, copy the modified letters to the Templates directory (listed above) and test them by printing from the Vendor Management Application. Additional modifications can be made as needed. The letter templates are written in Microsoft Word template using a mail merge. **Text in the letter template that is in << >> brackets is the mail merge value(s) and can never be deleted or modified without program changes.**

It is also very important to keep all Vendor Letters backed up to a CD or a backup directory on the server.

SPIRIT Vendor Form Letters

Letter Title	File Name
Applications	
Vendor Application	AP001
Vendor Application - Chain/Commissary	AP002
Vendor Application – Pharmacy	AP003
Vendor Application - Pharmacy Chain	AP004
Vendor Waiting List	AP005
Interim Application Letter	AP006
Application Approval	AP007
Application Denial	AP008
Expiration of Contract	AP009
Checks/Compliance Buys	
WIC Checks Submitted for Replacement - Redeposit	CH020
WIC Checks Submitted for Replacement - Not Replaced	CH021
Compliance Buy	CH022
Compliance Buy Meeting Letter	CH023
WIC Checks Submitted for Replacement - Redeposit	CH025
Disqualification	
Contract Termination - Store Closing	DQ040
Contract Termination - Change in Ownership	DQ041
Contract Termination - Withdrawal from Program	DQ042
Notification to Food Stamps of WIC Disqualification	DQ043
Disqualification Notification - Final Notice	DQ045
Monitoring	
Vendor Monitoring Visit	MN060
Onsite Warning	MN061

Notification General Information	
CPL Notification - CPL Survey	NG080
Stamps	
Vendor New Stamp	ST100
Vendor Replacement Stamp	ST101
Fee for Replacement of Lost Stamp	ST102
Training	
Annual Vendor Training	TR120
Special Training	TR122
Orientation Training	TR123
Vendor Training for All New Vendors	TR124
Make-up Vendor Training for New Vendors	TR125

We will use letter AP001.DOC and CH020.DOC as examples. The remainder of the letters should be modified using the same practices.

To Begin Updating:

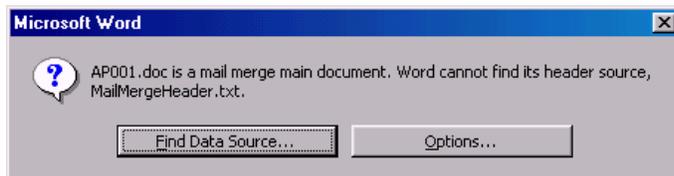
Double click on a letter to modify in your WORKING directory.

Example: Create directory C:\UPDATED VENDOR LETTERS on your local machine. Copy all letter templates from C:\Program Files\Covansys Inc. - BPDS\WIC\Templates to C:\UPDATED VENDOR LETTERS. Double click on any letter.

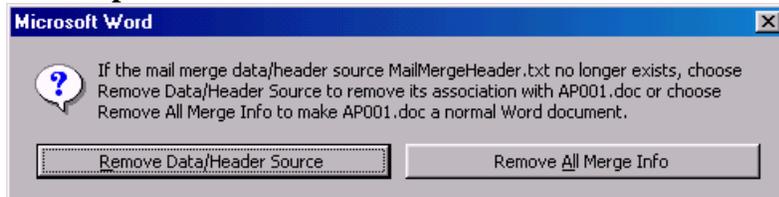
For this exercise, AP001.DOC is selected.

Note:

If you see this message



Click Options



Click Remove all Merge Info

The document will open in Microsoft Word.

You can now update this letter as you would any Microsoft word document.

It is important to leave all mail merge information intact.

Example 1:

In Letter AP001.DOC, the Header information can be deleted and replaced with any information you want to appear on your letterhead.



Just below the Header in the body of the document you will find the following information:

«LetterDate»

«Salutation» «FirstName» «LastName», «Title»

«Vendor»

«AddressLine1»

«AddressLine2»

«City», «ST» «ZIPCode»

SUBJECT: Vendor Application - Due Date Postmarked by April 15, 2000

Dear «Salutation» «LastName»:

The State Supplemental Nutrition Program for WIC is now accepting applications from retail food stores and pharmacies ...

The Subject line and the body of the letter can be changed. The bottom of this and all letters also include a mail merge value for <<userid>> to indicate who generated the letter. If this or any mail merge value is deleted, you may encounter errors when printing the letter.

Example 2:

Open the letter template CH020.DOC. This letter has mail merge values gathered in the body of the letter to include check numbers and issue dates for check that have been approved and require redeposit.

Check Number

«ReturnedCheck1»

«ReturnedCheck2»

«ReturnedCheck3»

«ReturnedCheck4»

«ReturnedCheck5»

Issue date

«IssueDate1»

«IssueDate2»

«IssueDate3»

«IssueDate4»

«IssueDate5»

In this letter you can change the text that is surrounding these mail merge values. Do not change any value within the <<>> brackets.

Move the letters to Templates folder:

Once you have completed updating the first letter, test it from the Vendor Management system. Copy the letter to the **C:\Program Files\Covansys Inc. - BPDSWIC\Templates** directory.

To test printing letter AP001.DOC from the Vendor application, open a Vendor folder for a Vendor who is independently owned. Click the Event Log tab of the Vendor Folder. Highlight the Applicant event in the Events tree view. Click the Details button. Click Send Application. Select a recipient and a mailing address. Click OK.

Review the letter and make additional modifications as necessary.

2.9 Maintenance and Backup

Recommended Monthly Server Maintenance:

We recommend Information Technology performs monthly server maintenance to install security patches and hot fixes, reboot systems, test fail-over and clean disk space. In case of emergency updates, the IT team should contact all effected personnel with time of expected updates to schedule a time for the updates with minimal production outage.

Recommended Server Backup Schedule:

The following is a recommended schedule of start times and duration of backup schedules:

- Differential backups should run daily Monday -Thursday evening.
- Full Backups should run each Friday evening.
- The 2nd Saturday of every month should be designated the Month-End Full backup.
- After completing Month-End processing for September, the 2nd Saturday of October should be designated the Year End Full backup.
- All backup tapes should be taken off-site daily to a secure facility.

Recommended retention times:

Daily's: 2 weeks

Full: 2 weeks

Month End: 1 year

Year End: Infinite

Recommended Database Backup Schedule:

Daily Database Server Maintenance

- Full database export backups of both database structure without data and database structure with data (Monday-Saturday).
- Full database hot backup (Monday-Saturday).
- Generate a script that will create the database with current structure.
- Update statistics on production schema objects (Monday-Friday).
- Every 15 minutes run a script that checks to see if database instance is up and page the on call DBA if it is down.
- Every 15 minutes run a series of database monitoring scripts and page the on call DBA if specific thresholds are exceeded.
- Every 30 minutes gather operating system performance metrics that can be used to troubleshoot database performance issues.
- Run SQL Server reports hourly to gather database performance metrics (Monday-Friday).
- Run a series of general database health monitoring scripts and email the results to the DBA group.
- Extract any SQL Server errors out of database alert log and email them to DBA team.

Weekly Database Server Maintenance

- A cold database backup should be performed every Sunday night.
- Compress database listener log and start new one during cold backup.
- Delete old logs and trace files.

Monthly Database Server Maintenance

- Compress database alert log and begin new one on the first day of each month.
- Reorganize any needed database objects.
- Apply any database patches as needed.

2.10 System Recovery

Individual Server Reboot:

5 servers can be rebooted at any time if no user is on the system.

- 1) SPIRITEOM01 - Application Server (EOM/EOD)
- 2) SPIRITMON01 (1) – Monitoring Server
- 3) SPIRITTST02 (2) – Testing Box
- 4) SPIRITFTP01 – FTP server

4 servers are load balanced so you would reboot one completely then the other.

- 1) SPIRITDC01 – Domain Controller
- 2) SPIRITDC02 – Domain Controller
- 3) SPIRITWEB01
- 4) SPIRITWEB02
- 5) SPIRITWEB03

2 Servers are clustered. SPIRITDB01 is currently being used so if a total reboot is needed, it would be SPIRITDB02. After it's completely up SPIRITDB01 can be rebooted and the cluster.

- 1) SPIRITDB01 - Database Server (1) will be set to fail over.
- 2) SPIRITDB02 - Database Server (2) will be set to fail over.

The Application server can be rebooted at any time as long as it is up and running before the EOM process or EOD process is to start running. **Do not** reboot this server during the EOM or EOD process.

The Raid Array **should not** have to be rebooted. If power or connection is lost, this would bring the entire system down. All data is stored in the Raid Array.

The FTP Server **should not** be rebooted during a transfer. If files were being transferred and the server is rebooted, the file **will not** be automatically resent.

The Database Servers should be set to fail over. If one Database Server was shut off, the end users should not notice anything. If both Database boxes lost power or connection at the same time this would bring the entire system down.

The test servers **do not** need to be rebooted.

If there is a planned update to the Data or Applications servers (Web/Application), reboot both DB servers and then reboot both Web servers. This process should be done after hours or with the knowledge that all users will be kicked off the system.

Entire System Shutdown:

1. If all servers need to go offline, you will want to do so in the following order:
2. Shutdown the web cluster servers first. You will want to bring one server down at a time. Wait until the servers are offline to ensure users don't have an active connection.
3. Shutdown the Application Server (EOD/EOM)
4. Shut down the MSSQL Server Cluster. You will want to turn off SERVER-X first, then turn off SERVER-Y

5. Shut down the Active Directory Servers

Entire System Startup:

1. The Active Directory servers should be started first.
2. After the AD servers are online, Turn on the MSSQL Servers and wait for each individual server to start before bringing the next server online.
3. Start the Application Server (EOD/EOM)
4. Turn on Web Servers one at a time; wait for each individual server to start before bringing the next server online.

Clustered Servers Troubleshooting:

Server Clusters: Backup and Recovery Best Practices for Windows Server 2003

Published: January 1, 2003

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/clustering/sercbrbp.mspx>

There are potentially two kinds of backups for Microsoft Windows Server 2003: An Authoritative System Restore (ASR) backup including the cluster configuration (we will refer to this as System State Backup) or a backup that is purely local (we will refer to this as a Local Backup). Note that to perform an Authoritative Restore, a System State Backup is required. If you perform an Authoritative Restore on one node, Microsoft recommends that you do a Non-Authoritative Restore on the other cluster nodes.

Cluster nodes fail to boot

In this case we assume that the quorum disk is functional and all of the data is intact.

One node in the cluster fails to boot

The other nodes in the cluster are running as expected.

Recommendation

Use Non-Authoritative Restore. This should work with either System State Backup or a local Backup.

This will result in the cluster database on the damaged node being restored and then the affected node should be able to re-join the cluster. In this case, it will download the most recent copy of the cluster database from the other nodes in the cluster.

All nodes in the cluster fail to boot

None of the cluster nodes are able to boot.

Recommendation

Use Non-Authoritative Restore on one node. Assuming the quorum disk is fine, the node should be able to form the cluster with the state on the quorum disk. If that does not work, then try the Authoritative Restore (this needs System State Backup) on the node.

Use Non-Authoritative Restore for all of the other nodes.

All nodes are fine but the quorum disk is not functional

The cluster nodes boot, but the cluster service cannot start on any of the nodes because it cannot bring the quorum resource online. An entry in the eventlog should point to the inability to bring the quorum online.

Recommendations

Replace the quorum disk if the drive itself has failed or reformat the quorum disk if the physical drive has not failed. Use an Authoritative Restore, if you have one, to bring up one node.

OR

Use the fixquorum flag to start the cluster service (note that fixquorum allows you to start the cluster service with a broken quorum resource that fails to come online but does not really fix any data for you) and chose an alternate quorum resource (local quorum can be used if you do not have another disk). By setting a new quorum, new quorum log files are created on the quorum but the registry checkpoint files are not restored because the old quorum is not available.

A Reskit tool ClusterRecovery is available to help with this procedure.

Follow the procedures in section Checkpoint files are lost or corrupt to address the checkpoint files.

Cluster database corruption on one of the Cluster Nodes

You can discover that this is the case if the node does not join and the entries in the cluster log (found at %windir%\cluster\cluster.log by default) point to a corrupted hive.

Recommendations

Do a Non-Authoritative Restore on this node and have it join the cluster

OR

Copy the latest checkpoint (chkXXX.tmp) file from the quorum disk and overwrite the file %windir%\cluster\clusdb on the affected node and restart the service.

OR

Stop the service on a working cluster node. Unload the cluster hive using RegEdit.

Copy the file %windir%\cluster\clusdb from the working node to %windir%\cluster\clusdb on the affected node, and restart the cluster service on all nodes.

All nodes were running fine but the quorum database became corrupt

In this case, no node is able to form the cluster and an entry in the eventlog points to a corrupt quorum log as the problem.

Recommendation

Start the cluster service with the resetquorumlogfile switch. If all of the resources start successfully and the configuration looks satisfactory then no action is required. By resetting the quorum, new quorum log files are created on the quorum disk but the registry checkpoint files are not restored because the old quorum is not available.

Follow the procedures in section Checkpoint files are lost or corrupt to address the checkpoint files.

If that fails, use Authoritative Restore on one node and restart the cluster service to form the cluster. Use Non-Authoritative Restore on other nodes.

Checkpoint files are lost or corrupt

If a registry checkpoint file is not found or cannot be loaded because it has been corrupted, resources may not have the most up-to-date information in the registry when they are brought online. The impact depends on the resource, however, in some cases; the resource may fail to come on line. In other cases, configuration changes that were made may be lost. If a checkpoint file is missing, the cluster service does not add an event to the event log, you will need to look at the cluster log if you suspect this is an issue.

Recommendation

If the resources fail to come online, use the resource kit tool ClusterRecovery to re-create the resource checkpoints.

Note: You should only restore the checkpoint files for resources that fail to come online.

If that does not solve the problem use Authoritative Restore on a cluster node and restart the cluster service to form the cluster. Use Non-Authoritative Restore on other nodes.

A cluster disk is corrupt or non functional

Resources that depend on this disk may not come online. The disk does not come online or the data on the disk is corrupt. There are two cases, either the disk needs to be replaced or it does not.

Disk itself is not corrupt and comes online

Recommendation

Restore the data to the disk

Disk is corrupt

Recommendations

Replace the disk and use a Non-Authoritative Restore on one node. Restore the data to the disk.

OR

Use the resource kit which contains a tool called ClusterRecovery which allows an existing physical disk resource to be replaced with a new disk without having to do a system state restore. Once the physical disk is brought online, you can restore any data.

Recovery without Backup of the System

In this case, we recommend procedures for troubleshooting some disaster scenarios without the use of a backup. The solution, for obvious reasons, may not be complete for all scenarios.
Single System Corruption of one or more Cluster Nodes

In this case, we assume that the quorum disk is functional and the data is intact.

One node in the cluster fails to boot the other cluster nodes are running as expected.

Recommendation

Evict that node and try to find a replacement.

Join the new node to the cluster.

All nodes in the cluster are dead

Recommendation

You will have to rebuild the cluster from scratch.

All nodes are fine but the quorum disk is not functional

Recommendation

Use the fixquorum flag to start the cluster service (note that fixquorum allows you to start the cluster service with a broken quorum resource that fails to come online but does not really fix any data for you) and chose an alternate quorum resource (local quorum can be used if you do not have another disk). By setting a new quorum, new quorum log files are created on the quorum but the registry checkpoint files are not restored because the old quorum is not available.

A Reskit tool ClusterRecovery is available to help with this procedure. Follow the procedures in section Checkpoint files are lost or corrupt to address the checkpoint issue.

The cluster database is corrupt on one of the Cluster Nodes

Recommendation

Copy the latest checkpoint (chkXXX.tmp) file from the quorum disk and overwrite the file %windir%\cluster\clusdb on the affected node and restart the cluster service.

OR

Stop the service on another node. Unload the cluster hive using RegEdit.

Copy the file %windir%\cluster\clusdb from one of running nodes in the cluster to %windir%\cluster\clusdb on the affected node and restart the cluster service on all nodes.

All nodes were running fine but the quorum database became corrupt

Recommendation

Start the cluster service with the resetquorumlogfile switch. If all of the resources start successfully and configuration looks satisfactory then no action is required. By resetting the quorum, new quorum log files are created on the quorum disk but the registry checkpoint files are not restored because the old quorum is not available.

Follow the procedures in section Checkpoint files are lost or corrupt to address the checkpoint files.

Checkpoint files are lost or corrupt

If a registry checkpoint file is not found or cannot be loaded because it has been corrupted, resources may not have the most up-to-date information in the registry when they are brought online. The impact depends on the resource, however, in some cases; the resource may fail to come on line. In other cases, configuration changes that were made may be lost. If a checkpoint file is missing, the cluster service does not add an event to the event log, you will need to look at the cluster log if you suspect this is an issue.

Recommendation

If the resources fail to come online, use the resource kit tool ClusterRecovery to re-create the resource checkpoints.

Note: You should only restore the checkpoint files for resources that fail to come online.

A cluster disk is corrupt or non functional

Recommendation

If the disk has been forcefully dismounted, it may require chkdsk to run in order to bring the disk online. The cluster service will run chkdsk automatically when the disk is brought online. In Windows Server 2003, a chkdsk log is preserved so that you can see what state the disk is in and what issues were found. If the application data on the disk is corrupted or deleted and you do not have a backup, there is no way to recover the data. You will have to regenerate the data or re-build the application. Server clusters does not provide user data protection and redundancy, you should use redundant hardware (mirrored disks or RAID disks) and take frequent backups of the data.

2.11 Environment and Security

We highly recommend a secure environment for servers and networking components, as well as a security policy for application access. Servers can be physically secured with the use of a lock system that requires security cards or biometric access

The optimum range for users that need to work in the server room, and equipment reliability, is normally between 68 to 74 degrees Fahrenheit. Aim to avoid temperature changes greater than 10 degrees F per hour and humidity changes of + or -10% in the same period. A relative humidity level between 45% and 60% are best for safe server operation and minimizes risk from static electricity.

Network Security Policy: Best Practices White Paper

<http://www.cisco.com/warp/public/126/secpol.html#t1>

Introduction

Without a security policy, the availability of your network can be compromised. The policy begins with assessing the risk to the network and building a team to respond. Continuation of the policy requires implementing a security change management practice and monitoring the network for security violations. Lastly, the review process modifies the existing policy and adapts to lessons learned.

This document is divided into three areas: preparation, prevention, and response. Let's look at each of these steps in detail.

Preparation

Prior to implementing a security policy, you must do the following:

- Create usage policy statements.
- Conduct a risk analysis.
- Establish a security team structure.

Create Usage Policy Statements

We recommend creating usage policy statements that outline users' roles and responsibilities with regard to security. You can start with a general policy that covers all network systems and data within your company. This document should provide the general user community with an understanding of the security policy, its purpose, guidelines for improving their security practices, and definitions of their security responsibilities. If your company has identified specific actions that could result in punitive or disciplinary actions against an employee, these actions and how to avoid them should be clearly articulated in this document.

The next step is to create a partner acceptable use statement to provide partners with an understanding of the information that is available to them, the expected disposition of that information, as well as the conduct of the employees of your company. You should clearly explain any specific acts that have been identified as security attacks and the punitive actions that will be taken should a security attack be detected.

Lastly, create an administrator acceptable use statement to explain the procedures for user account administration, policy enforcement, and privilege review. If your company has specific policies concerning user passwords or subsequent handling of data, clearly present those policies as well. Check the policy against the partner acceptable use and the user acceptable use policy statements to ensure uniformity. Make sure that administrator requirements listed in the acceptable use policy are reflected in training plans and performance evaluations.

Conduct a Risk Analysis

A risk analysis should identify the risks to your network, network resources, and data. This doesn't mean you should identify every possible entry point to the network, nor every possible means of attack. The intent of a risk analysis is to identify portions of your network, assign a threat rating to each portion, and apply an appropriate level of security. This helps maintain a workable balance between security and required network access.

Assign each network resource one of the following three risk levels:

- Low Risk Systems or data that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would not disrupt the business or cause legal or financial ramifications. The targeted system or data can be easily restored and does not permit further access of other systems.
- Medium Risk Systems or data that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would cause a moderate disruption in the business, minor legal or financial ramifications, or provide further access to other systems. The targeted system or data requires a moderate effort to restore or the restoration process is disruptive to the system.
- High Risk Systems or data that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would cause an extreme disruption in the business, cause major legal or financial ramifications, or threaten the health and safety of a person. The targeted system or data requires significant effort to restore or the restoration process is disruptive to the business or other systems.

Assign a risk level to each of the following: core network devices, distribution network devices, access network devices, network monitoring devices (SNMP monitors and RMON probes), network security devices (RADIUS and TACACS), e-mail systems, network file servers, network print servers, network application servers (DNS and DHCP), data application servers (SQL Server or other standalone applications), desktop computers, and other devices (standalone print servers and network fax machines).

Network equipment such as switches, routers, DNS servers, and DHCP servers can allow further access into the network, and are therefore either medium or high risk devices. It is also possible that corruption of this equipment could cause the network itself to collapse. Such a failure can be extremely disruptive to the business.

Once you've assigned a risk level, it's necessary to identify the types of users of that system. The five most common types of users are:

- Administrator's internal users responsible for network resources.
- Privileged internal users with a need for greater access.
- Internal users with general access.
- Partners External users with a need to access some resources.
- Others External users or customers.

The identification of the risk level and the type of access required of each network system forms the basis of the following security matrix. The security matrix provides a quick reference for each system and a starting point for further security measures, such as creating an appropriate strategy for restricting access to network resources.

System	Description	Risk Level	Types of Users
ATM switches	Core network device	High	Administrators for device configuration (support staff only); All others for use as a transport
Network routers	Distribution network device	High	Administrators for device configuration (support staff only); All others for use as a transport
Closet switches	Access network device	Medium	Administrators for device configuration (support staff only); All others for use as a transport
ISDN or dial up servers	Access network device	Medium	Administrators for device configuration (support staff only); Partners and privileged users for special access
Firewall	Access network device	High	Administrators for device configuration (support staff only); All others for use as a transport
DNS and DHCP servers	Network applications	Medium	Administrators for configuration; General and privileged users for use
External e-mail server	Network application	Low	Administrators for configuration; All others for mail transport between the Internet and the internal mail server
Internal e-mail server	Network application	Medium	Administrators for configuration; All other internal users for use
SQL Server database	Network application	Medium or High	Administrators for system administration; Privileged users for data updates; General users for data access; All others for partial data access

Establish a Security Team Structure

Create a cross-functional security team led by a Security Manager with participants from each of your company's operational areas. The representatives on the team should be aware of the security policy and the technical aspects of security design and implementation. Often, this requires additional training for the team members. The security team has three areas of responsibilities: policy development, practice, and response.

Policy development is focused on establishing and reviewing security policies for the company. At a minimum, review both the risk analysis and the security policy on an annual basis.

Practice is the stage during which the security team conducts the risk analysis, the approval of security change requests, reviews security alerts from both vendors and the CERT leavingcisco.com CERT mailing list, and turns plain language security policy requirements into specific technical implementations.

The last area of responsibility is response. While network monitoring often identifies a security violation, it is the security team members who do the actual troubleshooting and fixing of such a violation. Each security team member should know in detail the security features provided by the equipment in his or her operational area.

While we have defined the responsibilities of the team as a whole, you should define the individual roles and responsibilities of the security team members in your security policy.

Prevention

Prevention can be broken into two parts: approving security changes and monitoring security of your network.

Approving Security Changes

Security changes are defined as changes to network equipment that have a possible impact on the overall security of the network. Your security policy should identify specific security configuration requirements in non-technical terms. In other words, instead of defining a requirement as "No outside sources FTP connections will be permitted through the firewall", define the requirement as "Outside connections should not be able to retrieve files from the inside network". You'll need to define a unique set of requirements for your organization.

The security team should review the list of plain language requirements to identify specific network configuration or design issues that meet the requirements. Once the team has created the required network configuration changes to implement the security policy, you can apply these to any future configuration changes. While it's possible for the security team to review all changes, this process allows them to only review changes that pose enough risk to warrant special treatment.

We recommend that the security team review the following types of changes:

- Any change to the firewall configuration.
- Any change to access control lists (ACL).
- Any change to Simple Network Management Protocol (SNMP) configuration.
- Any change or update in software that differs from the approved software revision level list.

We also recommend adhering to the following guidelines:

- Change passwords to network devices on a routine basis.
- Restrict access to network devices to an approved list of personnel.
- Ensure that the current software revision levels of network equipment and server environments are in compliance with the security configuration requirements.

In addition to these approval guidelines, have a representative from the security team sit on the change management approval board, in order to monitor all changes that the board reviews. The security team representative can deny any change that is considered a security change until it has been approved by the security team.

Monitoring Security of Your Network

Security monitoring is similar to network monitoring, except it focuses on detecting changes in the network that indicate a security violation. The starting point for security monitoring is determining what a violation is. In *Conduct a Risk Analysis*, we identified the level of monitoring required based on the threat to the system. In *Approving Security Changes*, we identified specific threats to the network. By looking at both these parameters, we'll develop a clear picture of what you need to monitor and how often.

In the Risk Analysis matrix, the firewall is considered a high-risk network device, which indicates that you should monitor it in real time. From the *Approving Security Changes* section, you see

that you should monitor for any changes to the firewall. This means that the SNMP polling agent should monitor such things as failed login attempts, unusual traffic, changes to the firewall, access granted to the firewall, and connections setup through the firewall.

Following this example, create a monitoring policy for each area identified in your risk analysis. We recommend monitoring low-risk equipment weekly, medium-risk equipment daily and high-risk equipment hourly. If you require more rapid detection, monitor on a shorter time frame.

Lastly, your security policy should address how to notify the security team of security violations. Often, your network monitoring software will be the first to detect the violation. It should trigger a notification to the operations center, which in turn should notify the security team, using a pager if necessary.

Response

Response can be broken into three parts: security violations, restoration, and review.
Security Violations

When a violation is detected, the ability to protect network equipment, determine the extent of the intrusion, and recover normal operations depends on quick decisions. Having these decisions made ahead of time makes responding to an intrusion much more manageable.

The first action following the detection of an intrusion is the notification of the security team. Without a procedure in place, there will be considerable delay in getting the correct people to apply the correct response. Define a procedure in your security policy that is available 24 hours a day, 7 days a week.

Next you should define the level of authority given to the security team to make changes, and in what order the changes should be made. Possible corrective actions are:

- Implementing changes to prevent further access to the violation.
- Isolating the violated systems.
- Contacting the carrier or ISP in an attempt to trace the attack.
- Using recording devices to gather evidence.
- Disconnecting violated systems or the source of the violation.
- Contacting the police, or other government agencies.
- Shutting down violated systems.
- Restoring systems according to a prioritized list.
- Notifying internal managerial and legal personnel.

Be sure to detail any changes that can be conducted without management approval in the security policy.

Lastly, there are two reasons for collecting and maintaining information during a security attack: to determine the extent to which systems have been compromised by a security attack, and to prosecute external violations. The type of information and the manner in which you collect it differs according to your goal.

To determine the extent of the violation, do the following:

- Record the event by obtaining sniffer traces of the network, copies of log files, active user accounts, and network connections.
- Limit further compromise by disabling accounts, disconnecting network equipment from the network, and disconnecting from the Internet.
- Backup the compromised system to aid in a detailed analysis of the damage and method of attack.
- Look for other signs of compromise. Often when a system is compromised, there are other systems or accounts involved.
- Maintain and review security device log files and network monitoring log files, as they often provide clues to the method of attack.

If you're interested in taking legal action, have your legal department review the procedures for gathering evidence and involvement of the authorities. Such a review increases the effectiveness of the evidence in legal proceedings. If the violation was internal in nature, contact your Human Resources department.

Restoration

Restoration of normal network operations is the final goal of any security violation response. Define in the security policy how you conduct, secure, and make available normal backups. As each system has its own means and procedures for backing up, the security policy should act as a meta-policy, detailing for each system the security conditions that require restoration from backup. If approval is required before restoration can be done, include the process for obtaining approval as well.

Review

The review process is the final effort in creating and maintaining a security policy. There are three things you'll need to review: policy, posture, and practice.

The security policy should be a living document that adapts to an ever-changing environment. Reviewing the existing policy against known Best Practices keeps the network up to date. Also, check the CERT web site leavingcisco.com CERT web site for useful tips, practices, security improvements, and alerts that can be incorporated into your security policy.

You should also review the network's posture in comparison with the desired security posture. An outside firm that specializes in security can attempt to penetrate the network and test not only the posture of the network, but the security response of your organization as well. For high-availability networks, we recommend conducting such a test annually.

Finally, practice is defined as a drill or test of the support staff to insure that they have a clear understanding of what to do during a security violation. Often, this drill is unannounced by management and done in conjunction with the network posture test. This review identifies gaps in procedures and training of personnel so that corrective action can be taken.

3.0 SITE OPERATIONS OVERVIEW

3.1 System Requirements

SPIRIT is best viewed by client PC utilizing Internet Explorer 5.5 or greater on Windows XP.

3.1.1 Maintenance Best Practices

To maintain optimal performance of Windows XP, the following steps should be taken.

- 1) Set Windows Update to Automatically download and install patches every night
- 2) Defrag your hard disk every week by selecting Start -> Programs -> Accessories -> System Tools -> Disk Defragmenter. Highlight your Hard Drive (usually c) and click the 'Defragment Button' at the bottom left of the window.
- 3) Schedule your Anti-Virus program to run a full scan nightly.
- 4) Install Anti-Spyware program if not included with your Antivirus – schedule to run a full scan nightly.

3.2 Communication Requirements

We recommend finding a local ISP provider to determine types of Internet connection speeds that are available at each site. Below is a list of recommended connections based on the number of simultaneous users, but not availability of service by ISP.

User Qty	ISP Service	Device
1-2	POTS / Dial Up	3COM LAN Modem
3-7	DSL / Cable	Cable/DSL Modem, Router/Switch with DHCP and Firewall
7 or more	Fractional T1 / T1	Router / Switch with DHCP and Firewall (possibly sourced from T1 Service Provider)

3.3 Troubleshooting FAQ

Q. I am unable to get to the SPIRIT website; I connected fine yesterday, what happened?

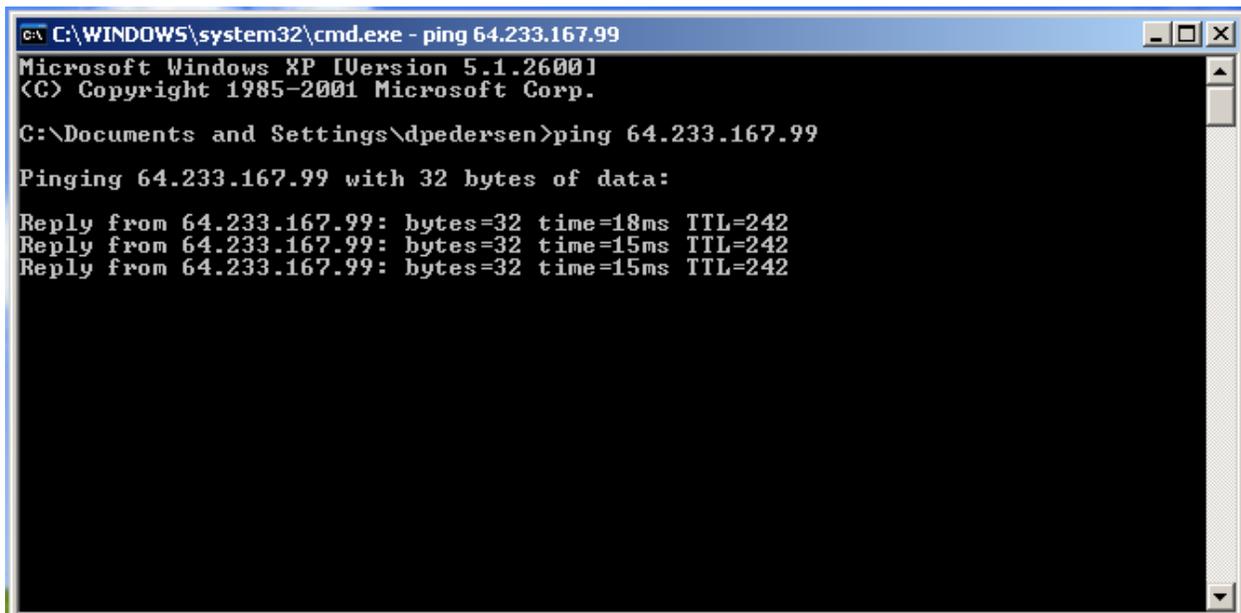
A. The first step is to see if you can connect to any other web sites with your web site browser, try going to www.google.com or www.yahoo.com.

If you can connect to those web sites, see if another computer in your office has trouble connecting to SPIRIT. If they are unable to connect, call the SPIRIT Help Desk Toll Free at 888-531-6780.

Ping Test

If you are unable to connect to other web sites, we will need to first do a ping test to check connectivity.

- Click 'Start' select 'Run' type 'CMD' and press the enter key.
- When you see the dos command prompt, type **ping 64.233.167.99** and hit enter
- If the response reads something like 'Reply from 64.233.167.99: bytes = 32 time=15ms TTL=242' you know you have a good network connection.
- Next try typing '**ping google.com**'. If the response reads something like 'Reply from 64.233.167.99: bytes = 32 time=15ms TTL=242' you know DNS is working. Try going to the SPIRIT web site again. If you are unsuccessful you should call the help desk.



```
C:\WINDOWS\system32\cmd.exe - ping 64.233.167.99
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\dpedersen>ping 64.233.167.99

Pinging 64.233.167.99 with 32 bytes of data:

Reply from 64.233.167.99: bytes=32 time=18ms TTL=242
Reply from 64.233.167.99: bytes=32 time=15ms TTL=242
Reply from 64.233.167.99: bytes=32 time=15ms TTL=242
```

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\dpedersen>ping google.com

Pinging google.com [64.233.167.99] with 32 bytes of data:

Reply from 64.233.167.99: bytes=32 time=42ms TTL=242
Reply from 64.233.167.99: bytes=32 time=50ms TTL=242
Reply from 64.233.167.99: bytes=32 time=15ms TTL=242
Reply from 64.233.167.99: bytes=32 time=16ms TTL=242

Ping statistics for 64.233.167.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 15ms, Maximum = 50ms, Average = 30ms

C:\Documents and Settings\dpedersen>
```

- When attempting to ping by IP address 24.233.167.99 or google.com you receive an error message that says 'Destination host unreachable', you are probably not connected to the internet.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\dpedersen>ping 24.233.167.99

Pinging 24.233.167.99 with 32 bytes of data:

Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.

Ping statistics for 24.233.167.99:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\dpedersen>_
```

Check the network cable in the back of your computer to ensure it's still plugged in. The network cable looks similar to a phone cable with a larger end. Please make sure this is pushed all the way in to the network card.



After plugging it in, you may see lights blinking in the back of your network card. If so, try the ping test again as described above.

If the ping test doesn't work, you may need to reset your Cable/DSL modem and router. Your office connects to the internet either by Telephone Modem, Cable or DSL Modem, or a special T-1 connection.

Telephone Modem

If you are connected by Telephone Modem, confirm that the AC adapter, phone cords, and network cables are all plugged in securely and into their assigned ports. Power cycle the modem by turning it off, or unplugging it. Wait 20 seconds then turn it back on. Click 'Start' select 'Run' type 'cmd' and hit the Enter key. Type `ipconfig/release` wait for a response, then click `ipconfig/renew`. Try again to connect to SPIRIT. If you are unable to connect to SPIRIT, and the ping test doesn't work, you will need to contact your help desk.

Cable or DSL Modem

If you are connected by Cable or DSL Modem, confirm that the AC adapter, phone cords, and network cables are all plugged in securely and into their assigned ports. Power cycle the cable/DSL modem by unplugging it. Next, turn off the accompanying router by unplugging it. Wait 20 seconds and plug in the cable/DSL modem, then plug in the router. After starting both back up, wait 20 seconds. Click 'Start' select 'Run' type 'cmd' and hit the Enter key. Type `ipconfig/release` wait for a response, then click `ipconfig/renew`. Try again to connect to SPIRIT. If you are unable to connect to SPIRIT, and the ping test doesn't work, you will need to contact your help desk.

T1 or Fractional T1

If you are connected through a T-1 or Fractional T-1 service, confirm that the AC adapter and network cables are all plugged in securely and into their assigned ports on the router. Power cycle the router by unplugging it. Wait 20 seconds and plug the router back in. Click 'Start' select 'Run' type 'cmd' and hit the Enter key. Type `ipconfig/release` and wait for a response, then click `ipconfig/renew`. Try again to connect to SPIRIT. If you are unable to connect to SPIRIT, and the ping test doesn't work, you will need to contact your help desk.

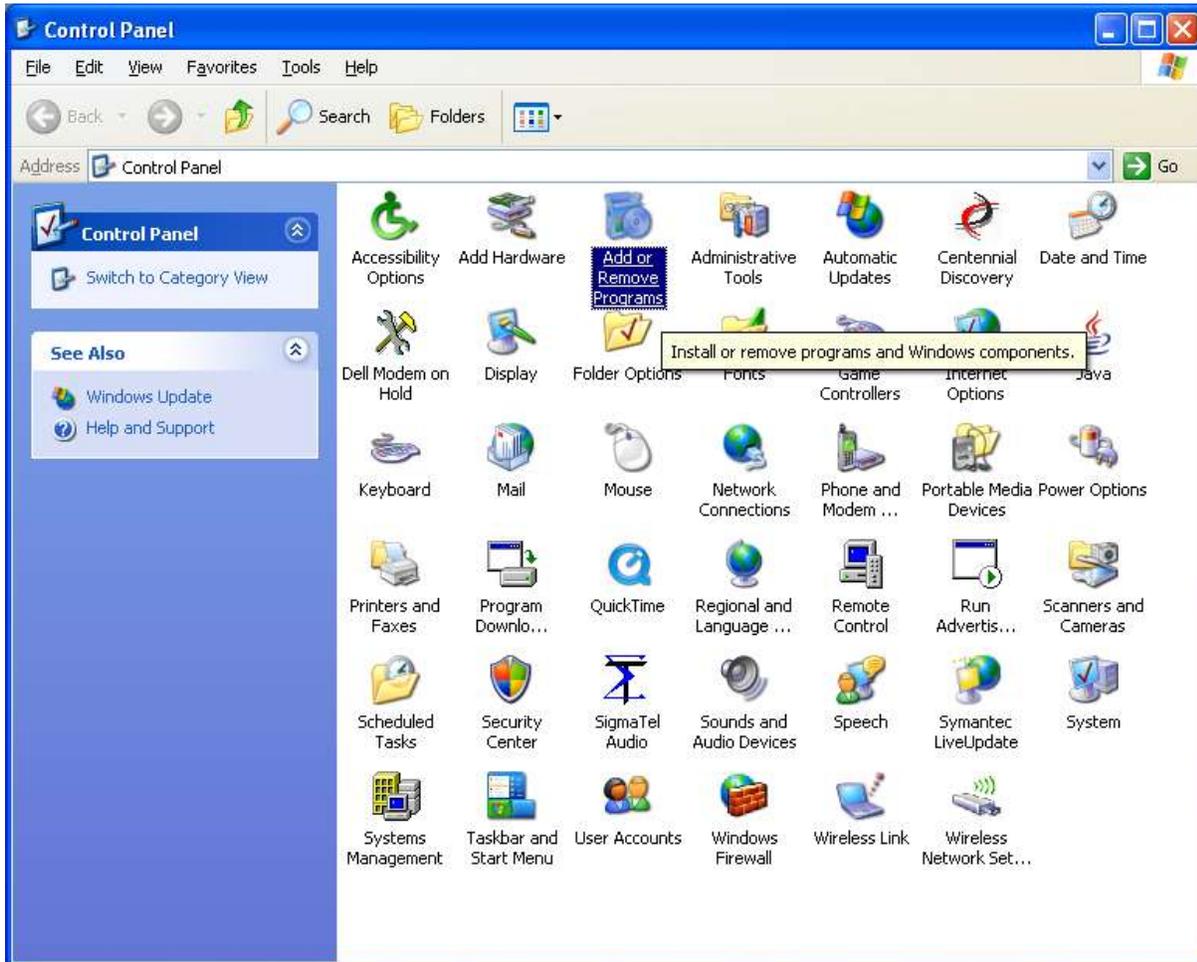
APPENDIX A

Installation Instructions

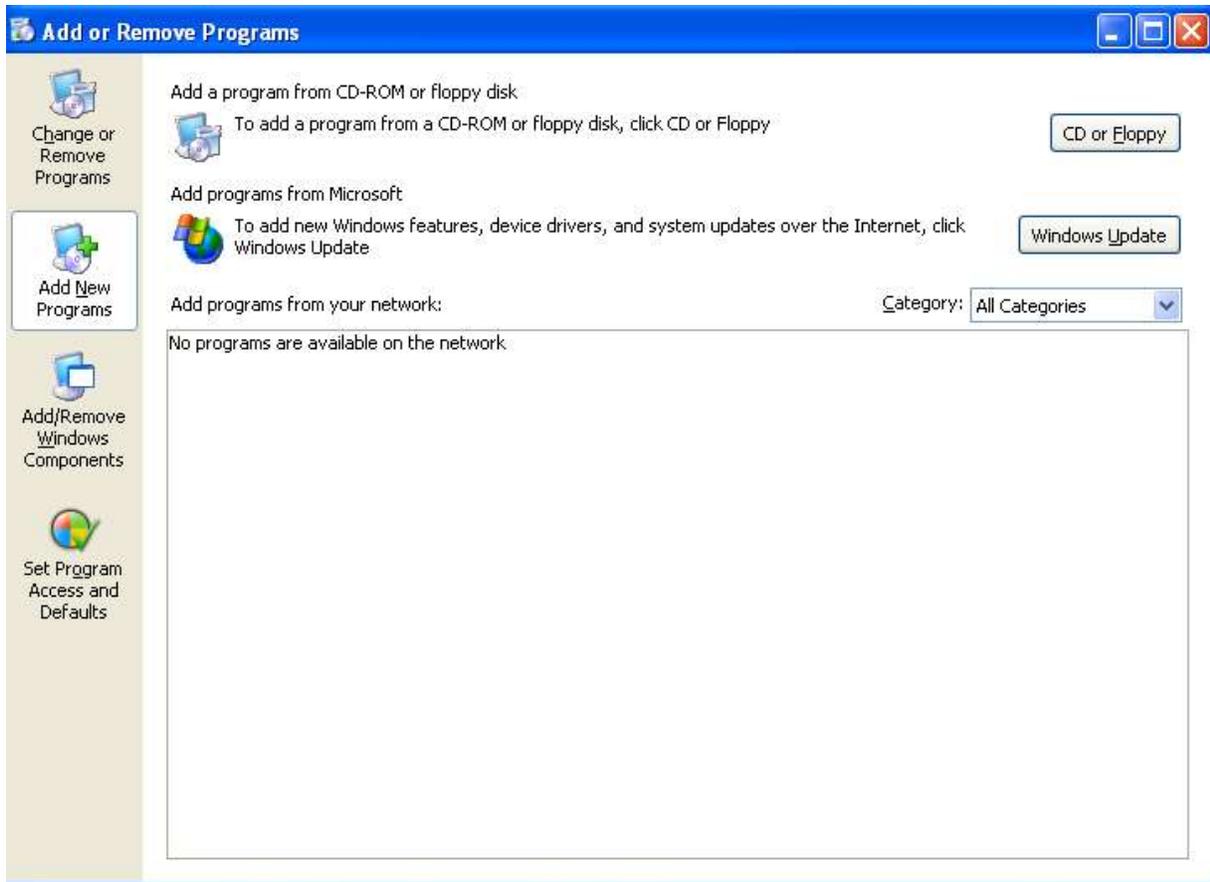
The following is a detailed description of the procedures that must be followed to complete the Spirit Installation process.

Web Server Install

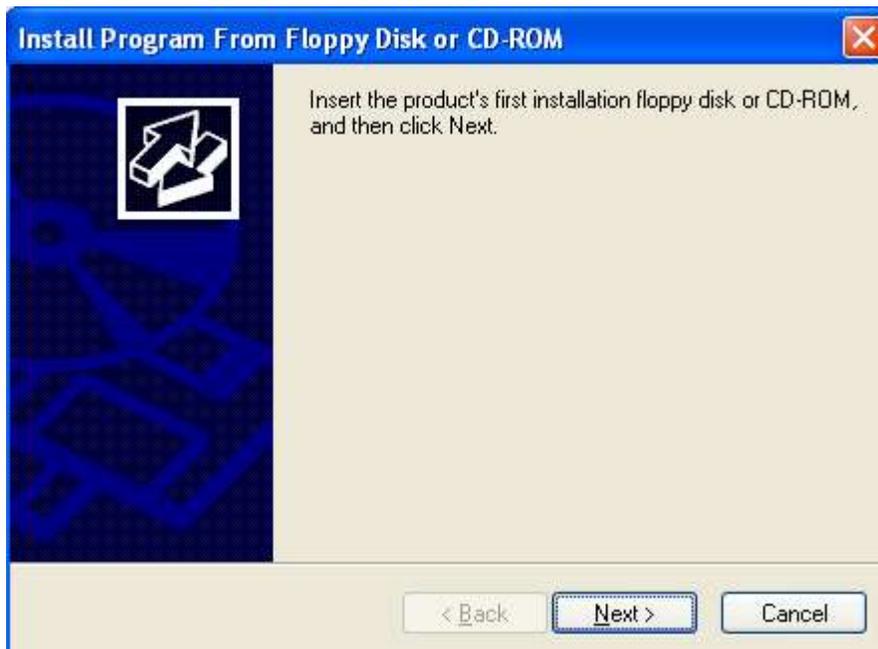
Open Add or Remove Programs from the control Panel



Click the Add New Programs button on the left then select the CD or Floppy button in the top right corner



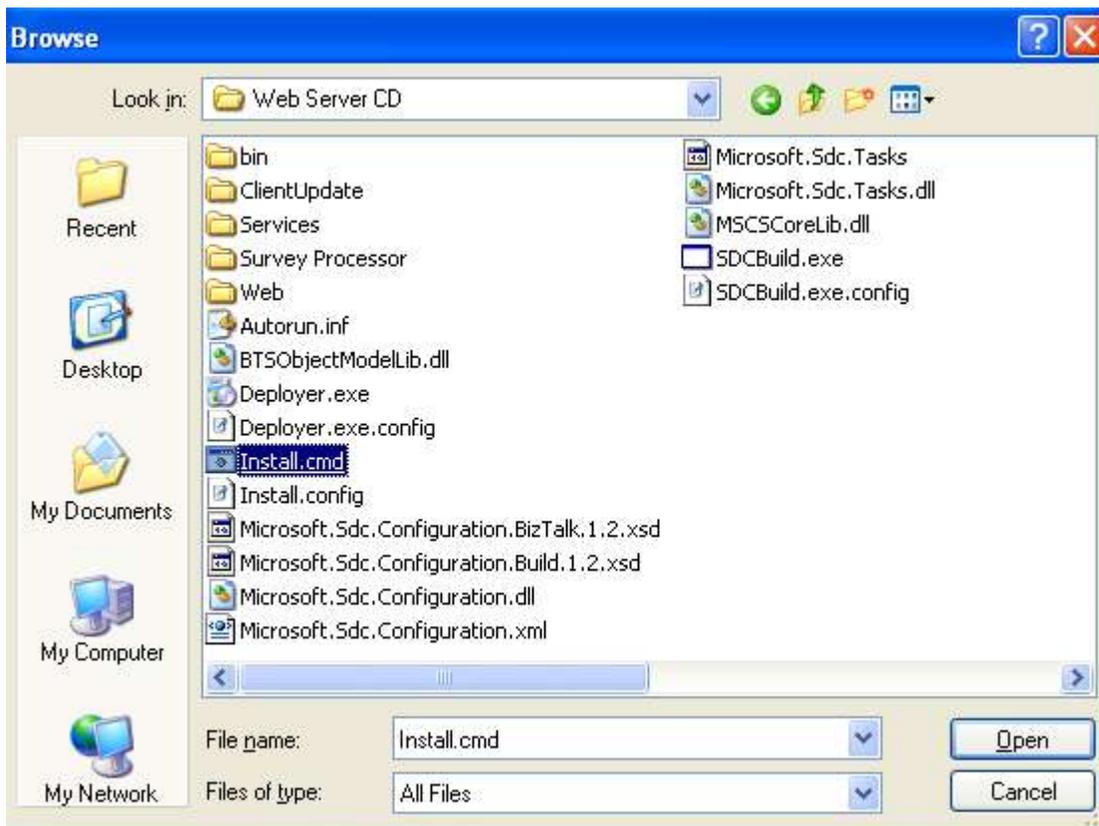
Click the Next button



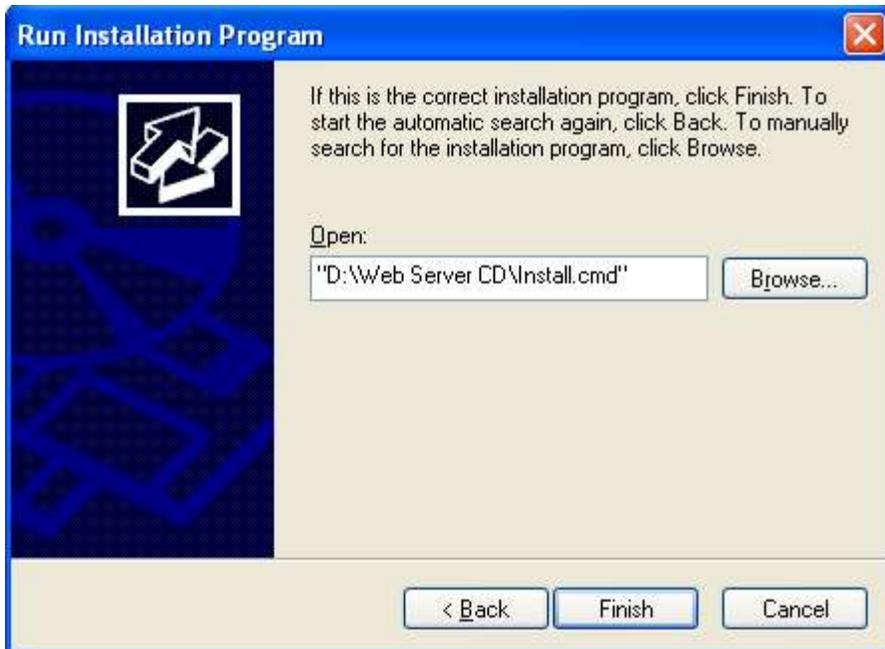
Now click the Browse button



Now find the Web Server folder on the CD and select the Install.cmd file and Click Open.
Note: the “Files of type” must be set to “All Files”



Now click Finish. This will start the install.



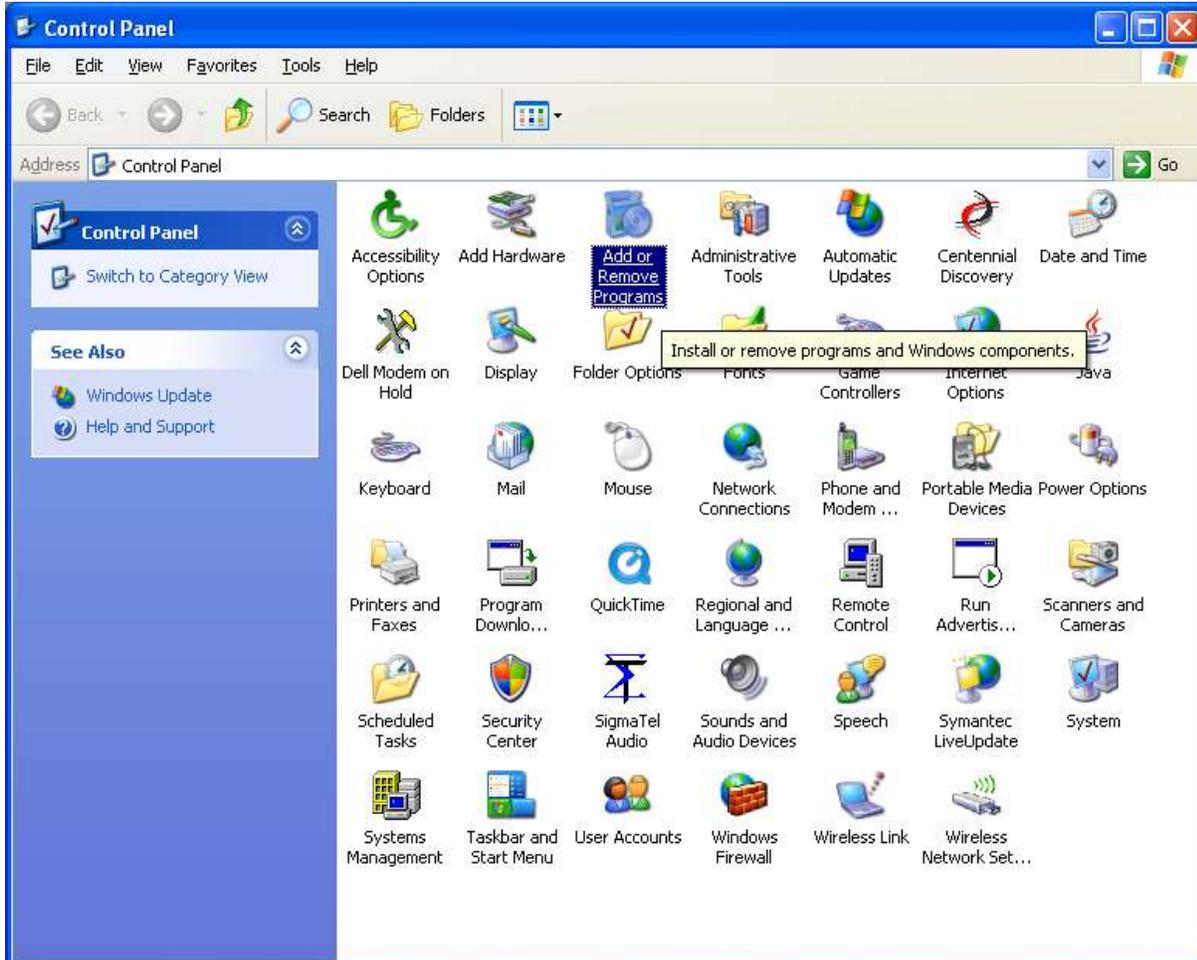
When the install is finished click "OK"



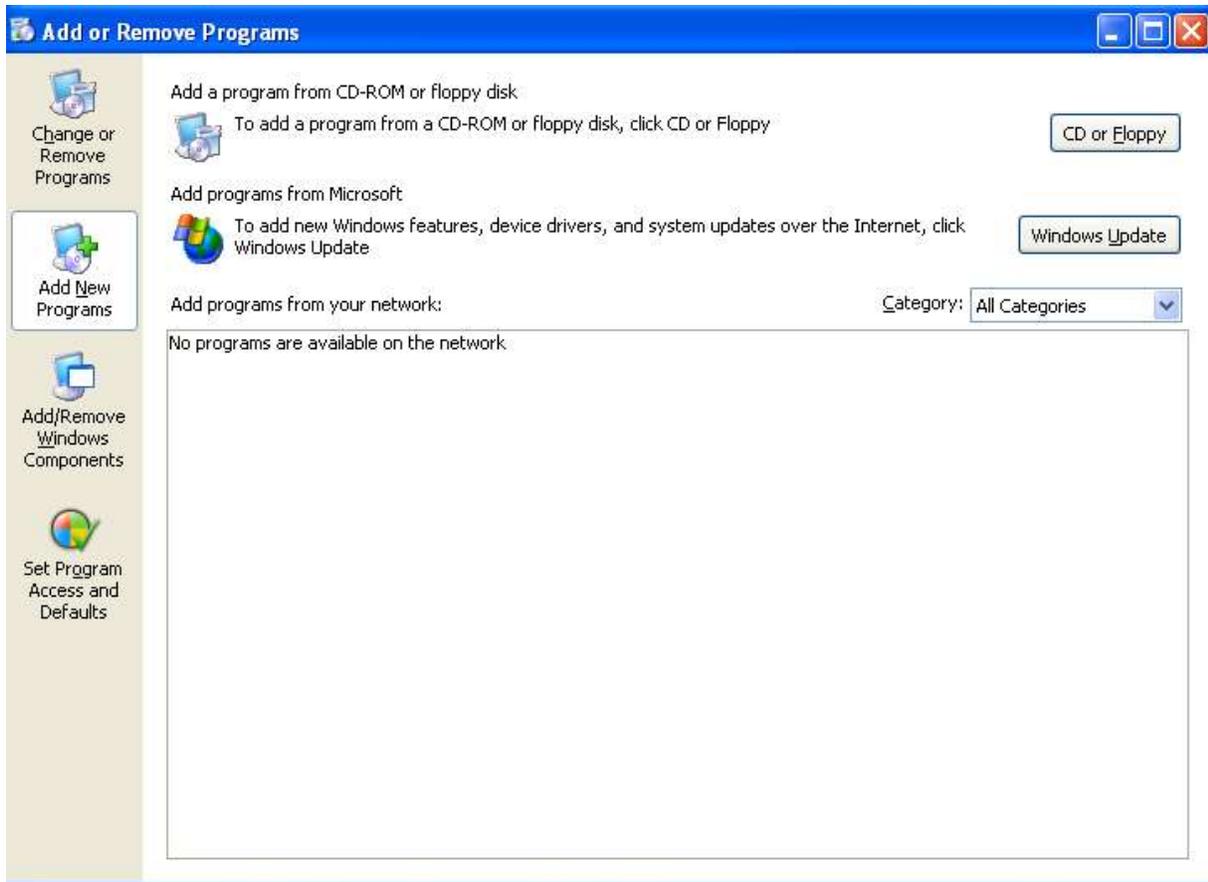
Client Install

This is for the initial install. After this install the client application will automatically check for updates on the web server.

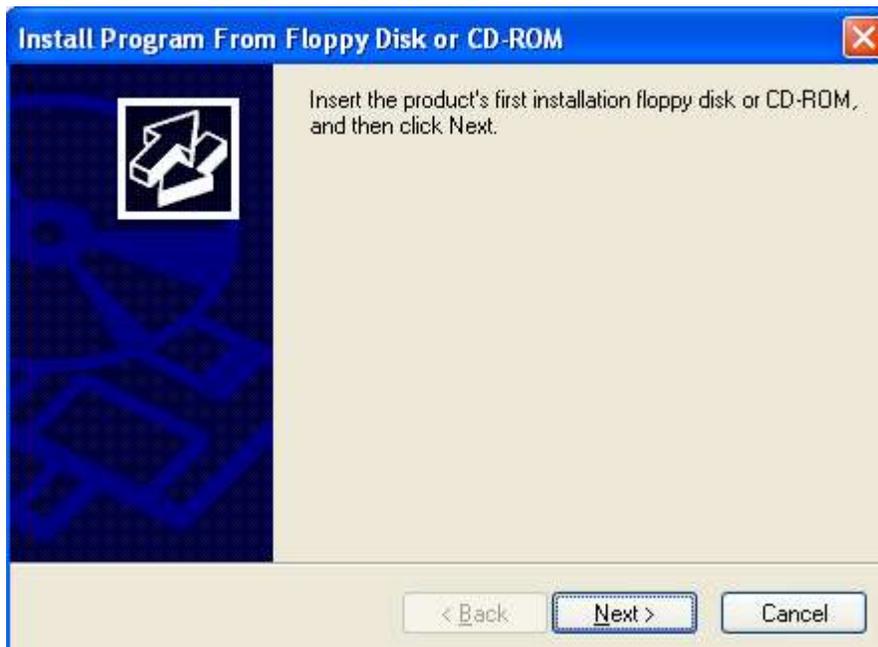
Open Add or Remove Programs from the control Panel



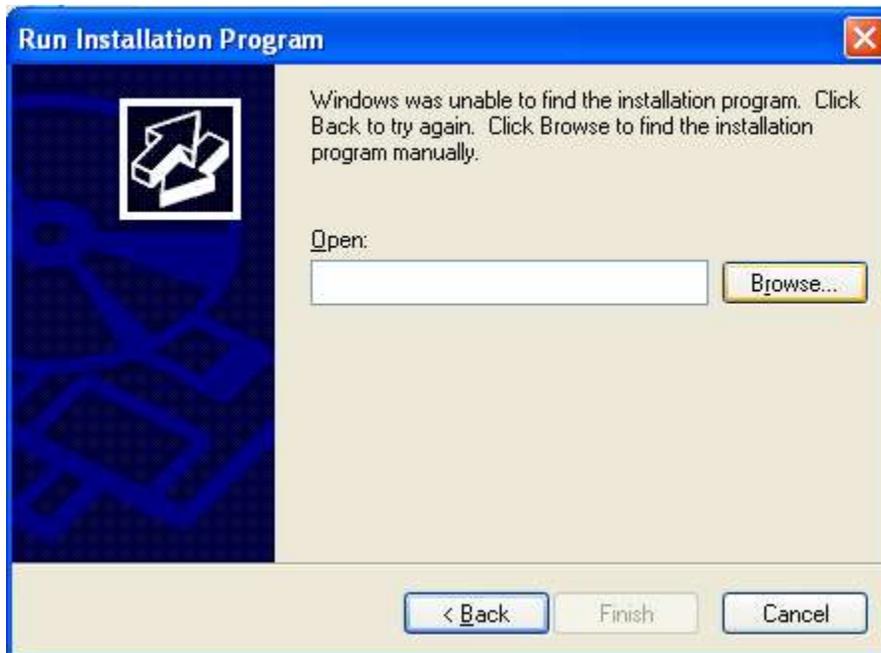
Click the Add New Programs button on the left then select the CD or Floppy button in the top right corner



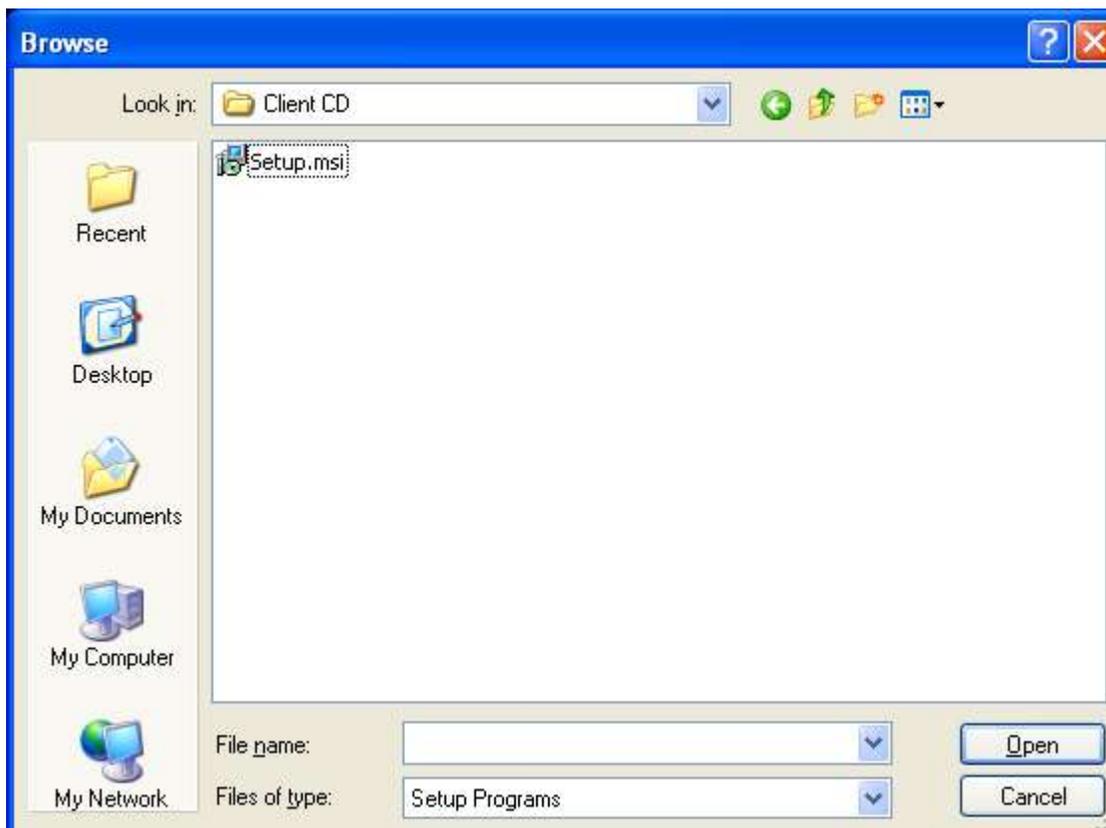
Click the Next button



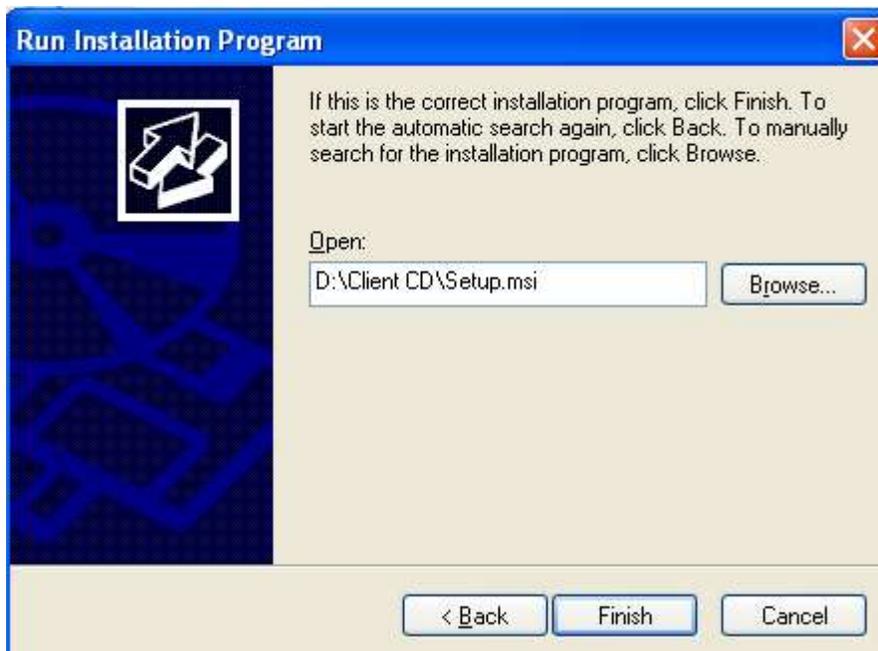
Now click the Browse button



Now find the Client folder on the CD and select the Setup.msi file and Click Open.



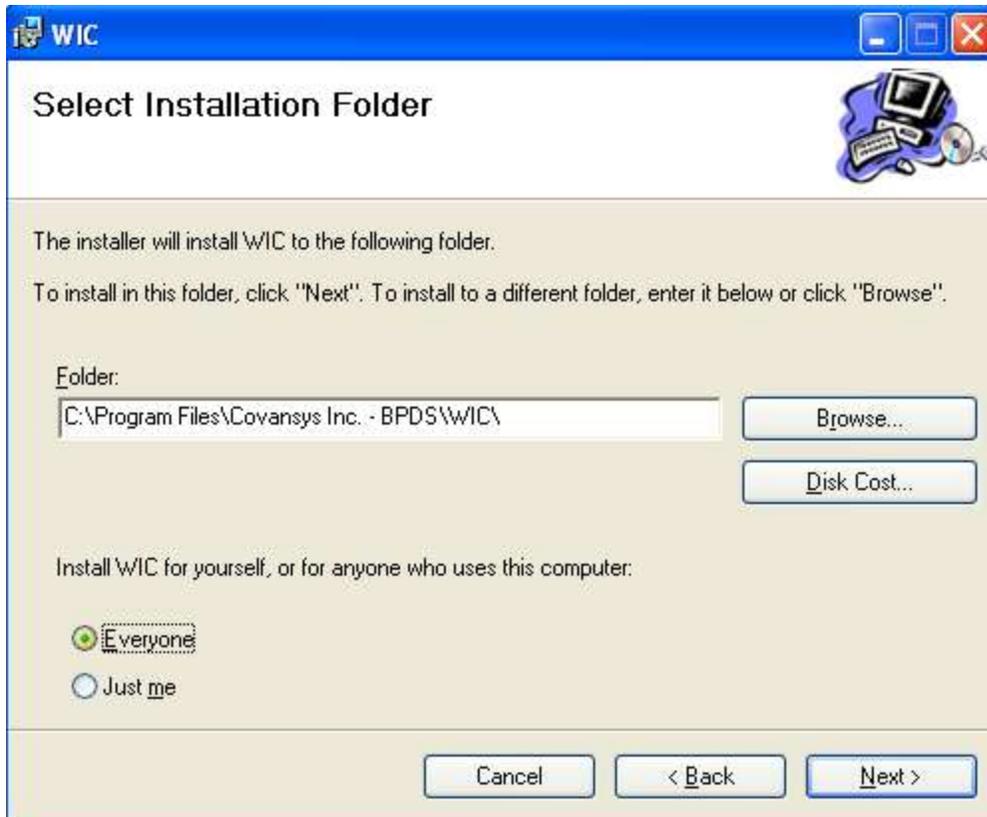
Now click Finish. This will start the install.



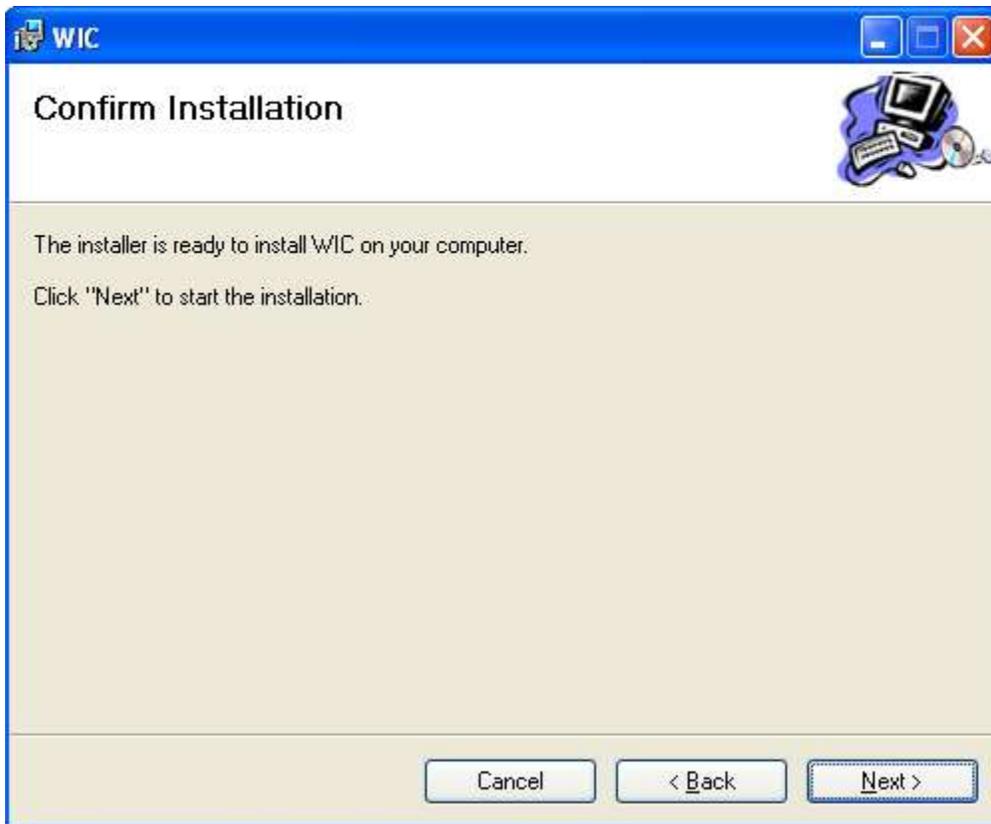
Click Next



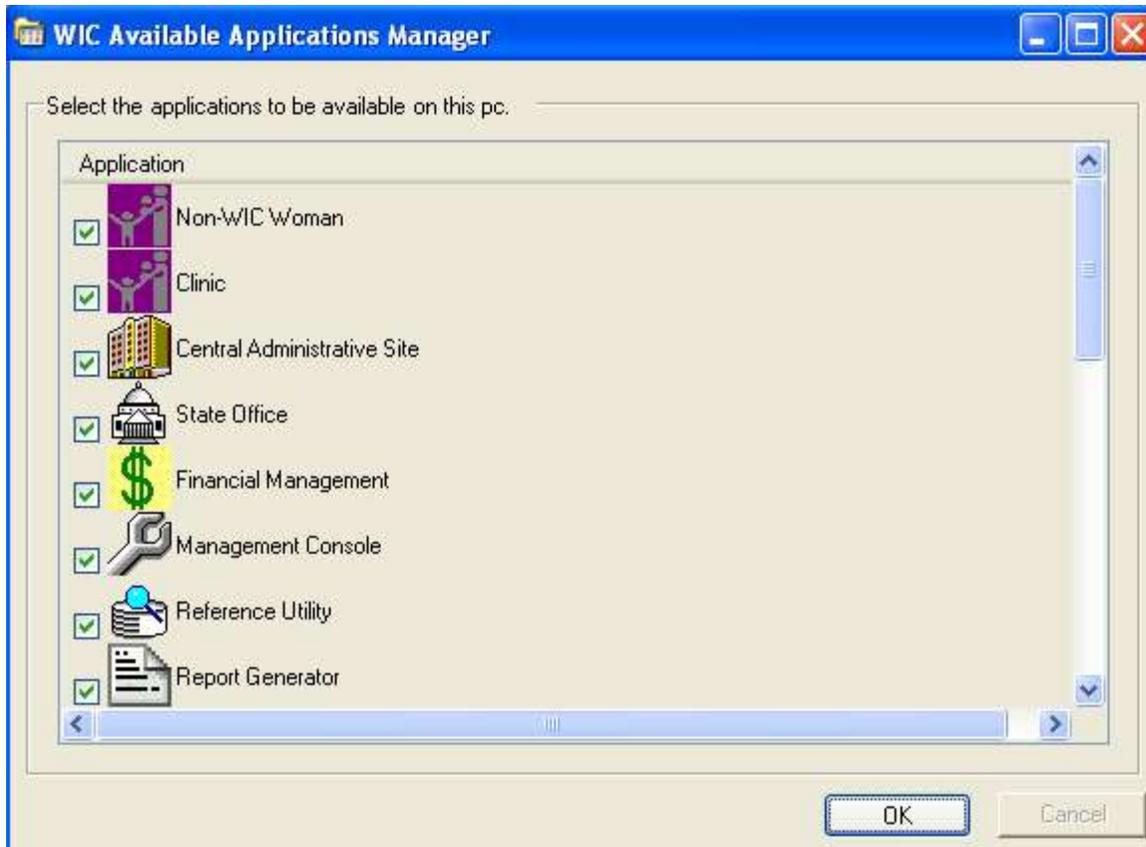
Click the “Everyone” and then click “Next”



Click Next button. This will start the install.



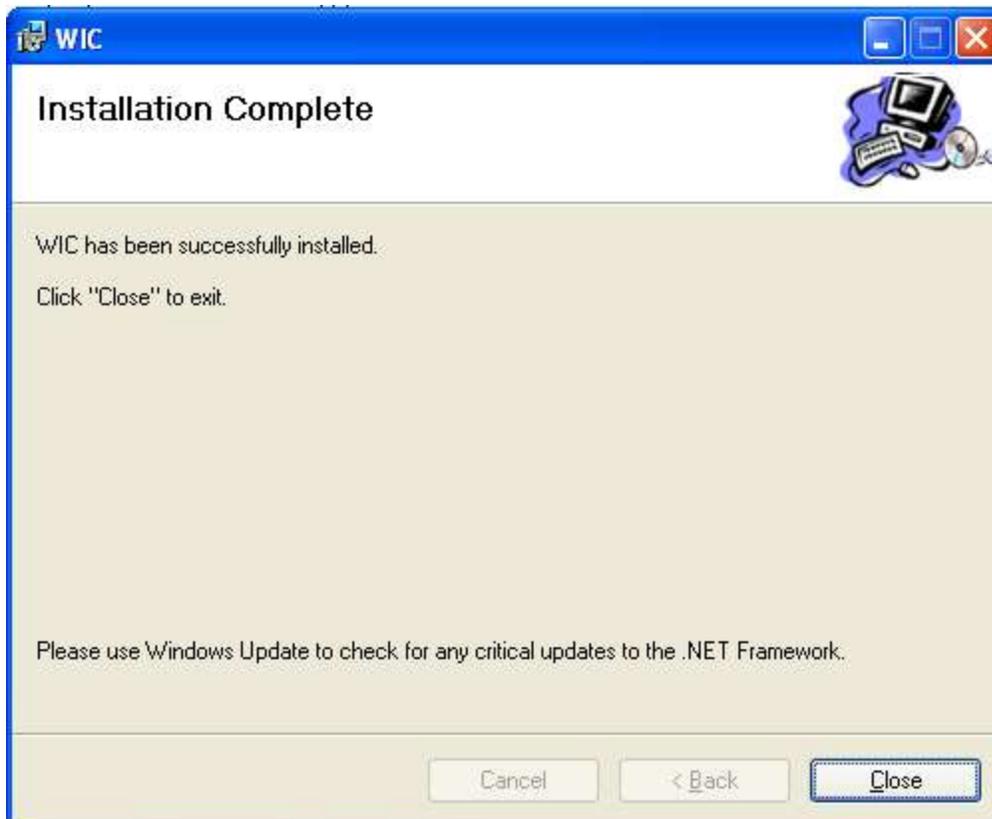
Select the applications to be available on the pc and then click OK



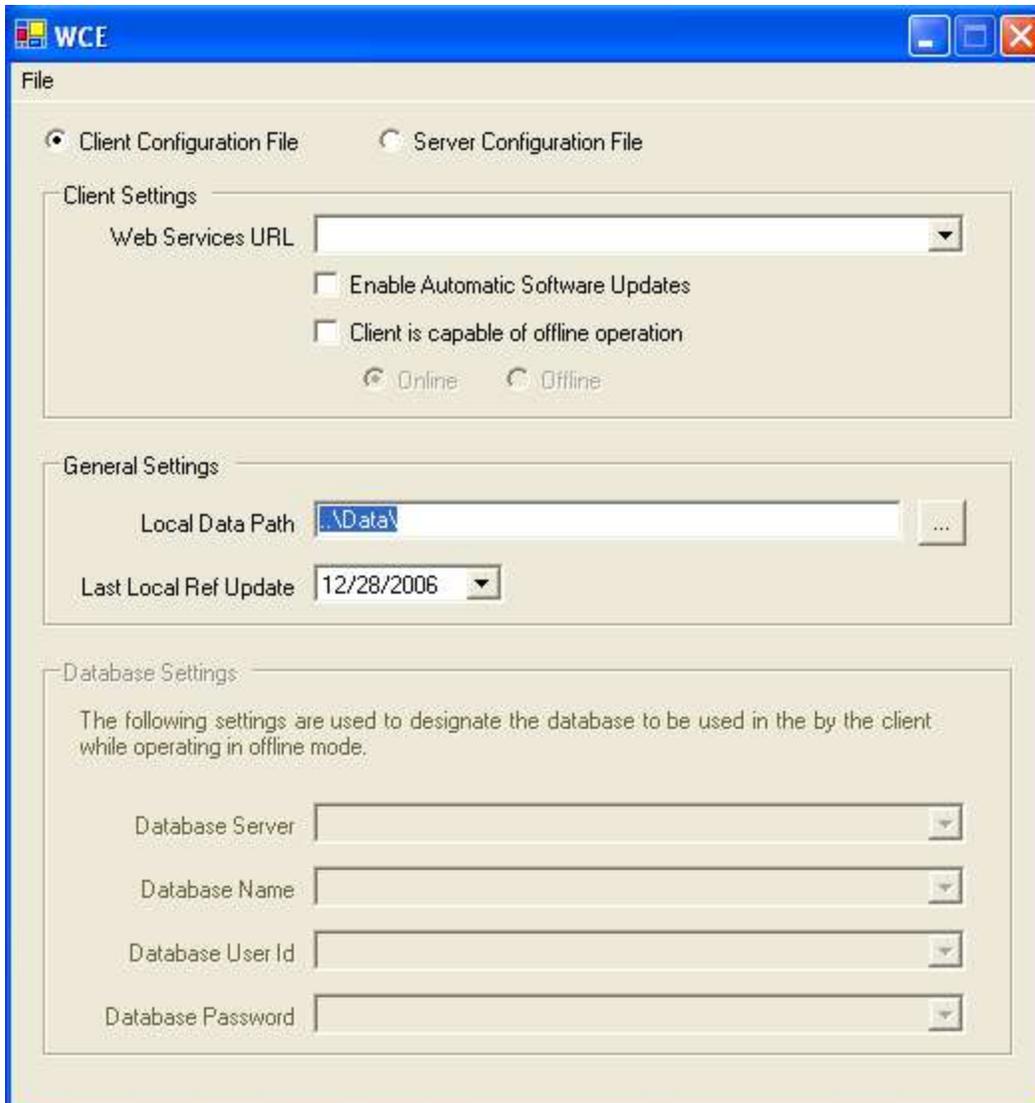
Click OK



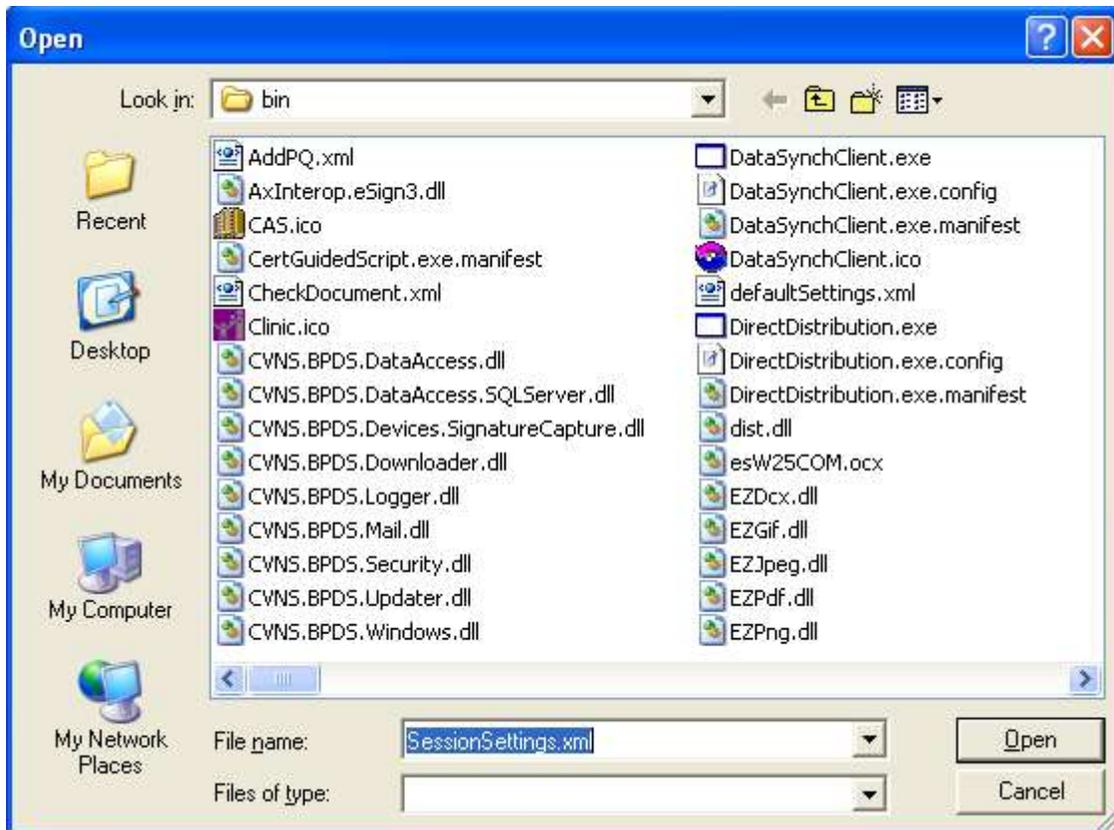
Click Close



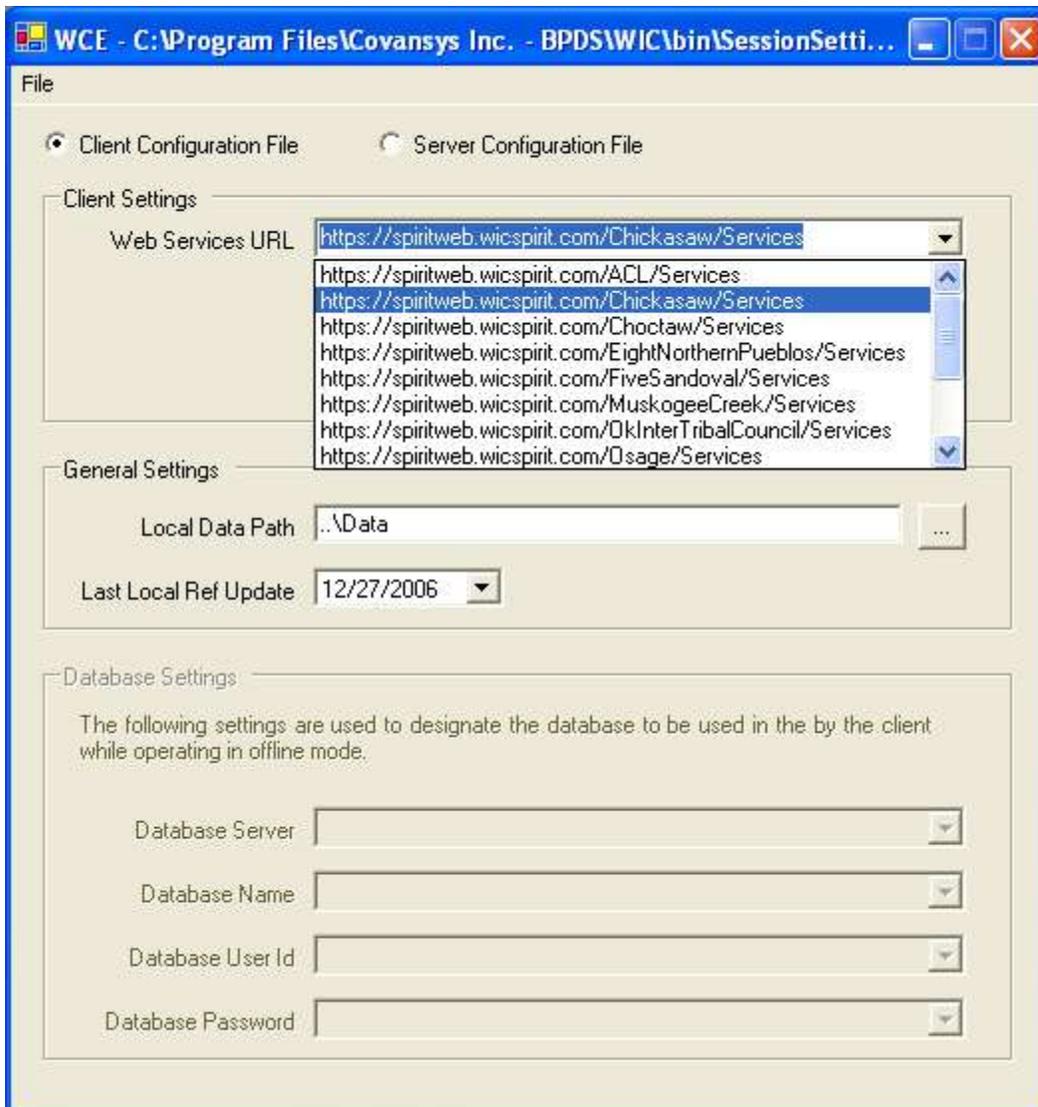
Once the install is complete open the WIC Config Editor. This is located in "Start -> All Programs -> WIC Applications -> WIC Config Editor" Select File -> Open from this screen.



Next click Open



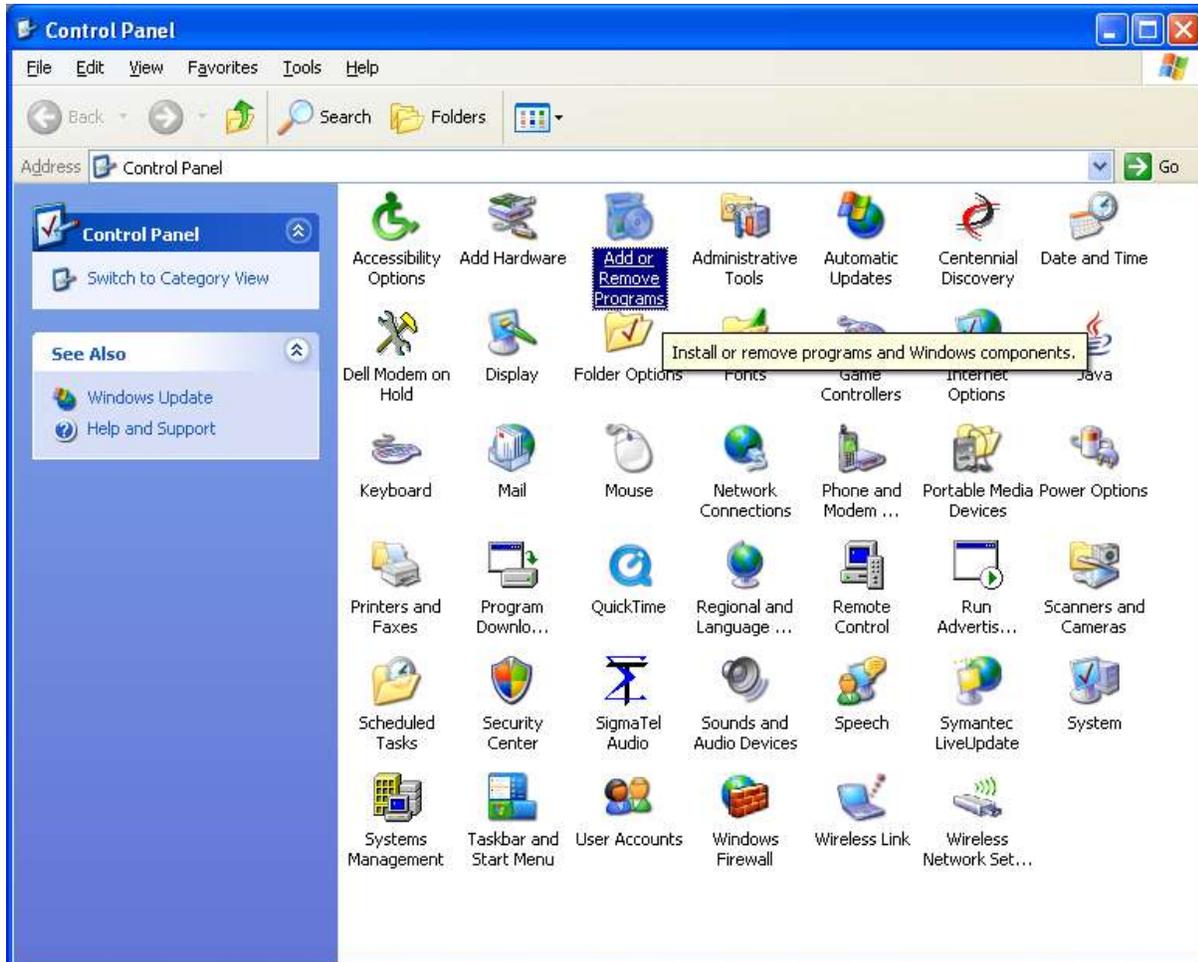
Next select the correct URL based on the State you wish to connect too. Once that is done click “File -> Save” and then exit.



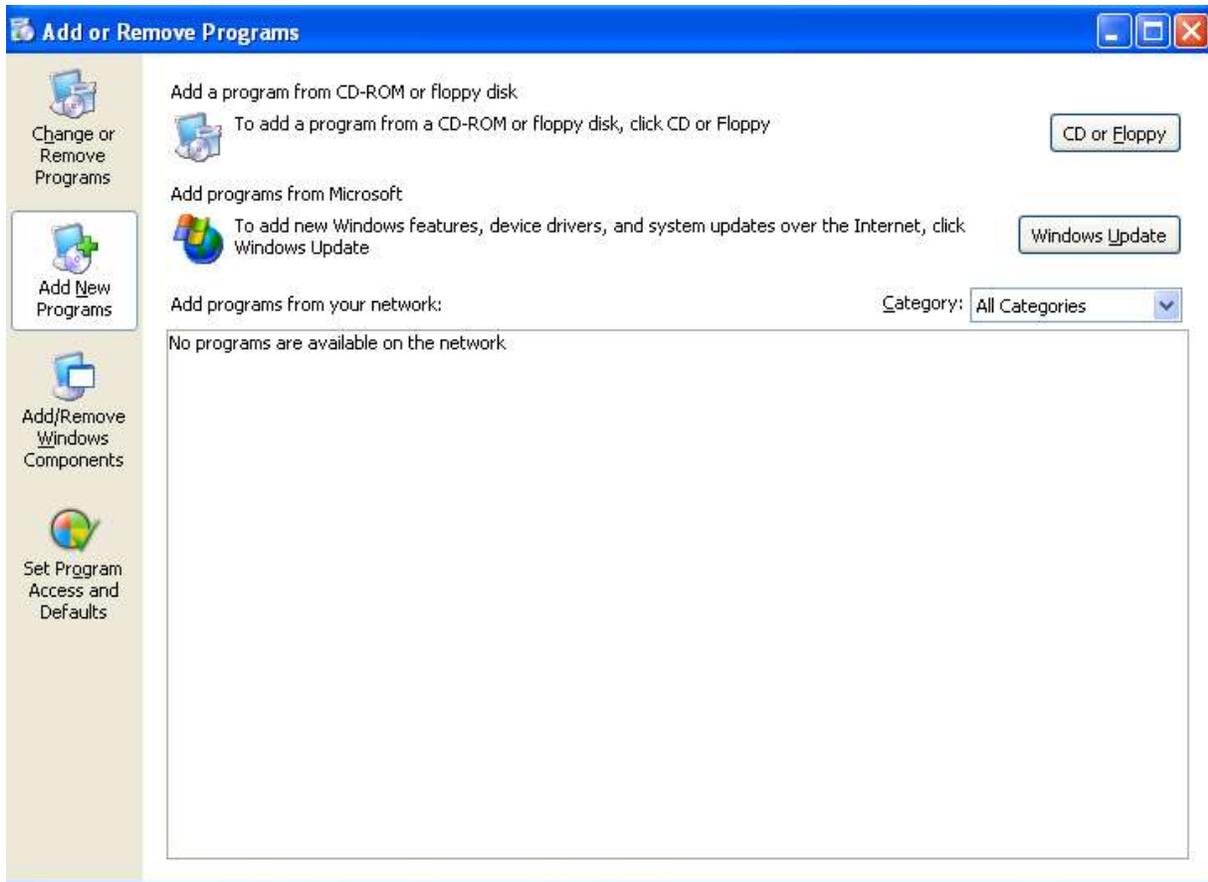
Application Server Install

For the first time setup the following bat file needs to be run: setup_dirs_app_server.bat

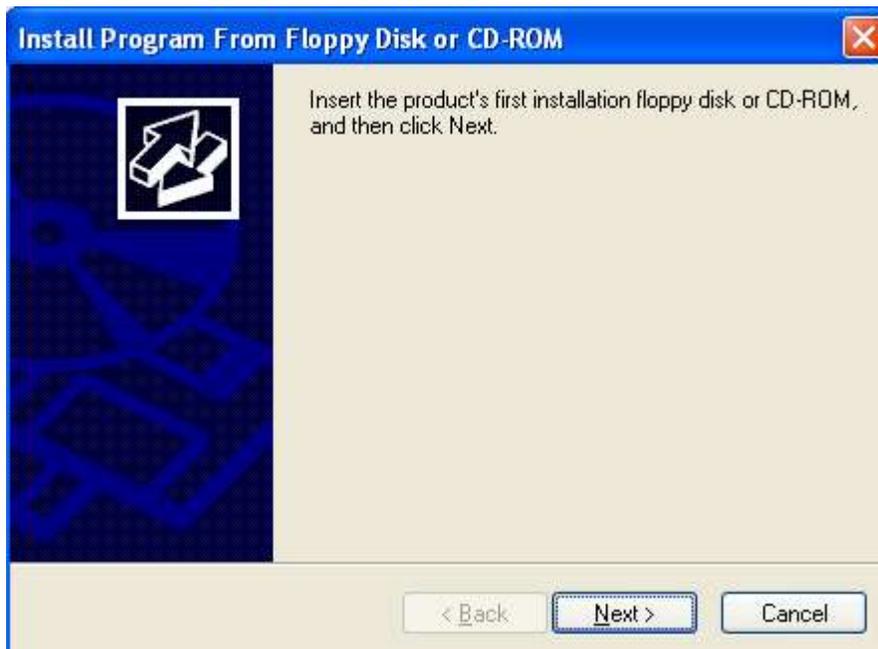
Open Add or Remove Programs from the control Panel



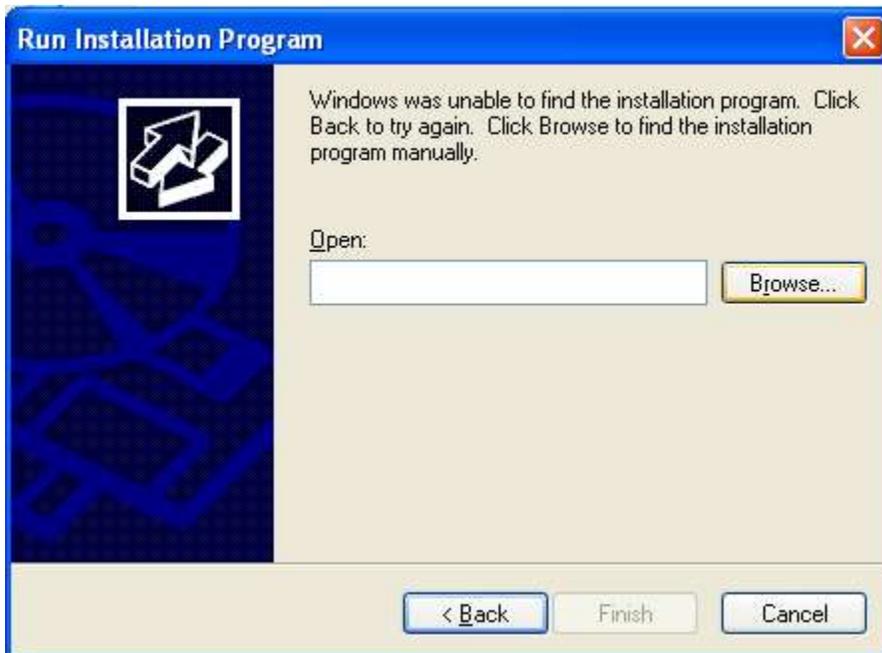
Click the Add New Programs button on the left then select the CD or Floppy button in the top right corner



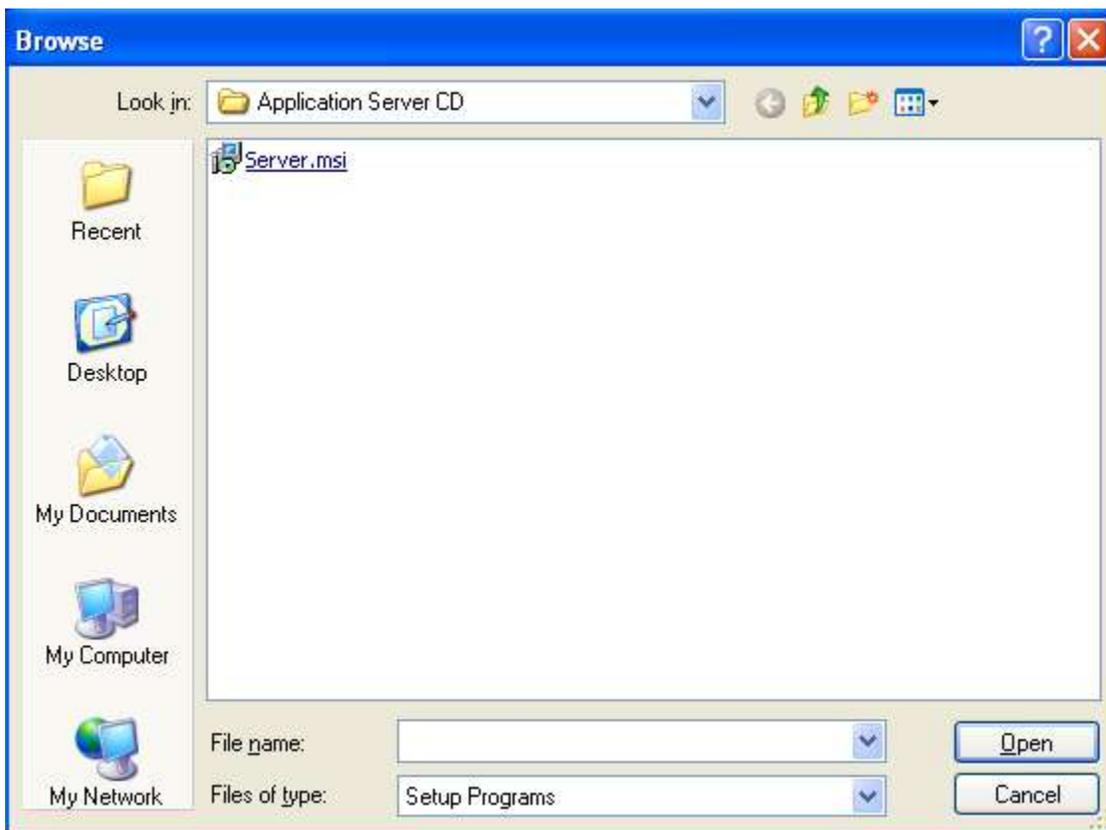
Click the Next button



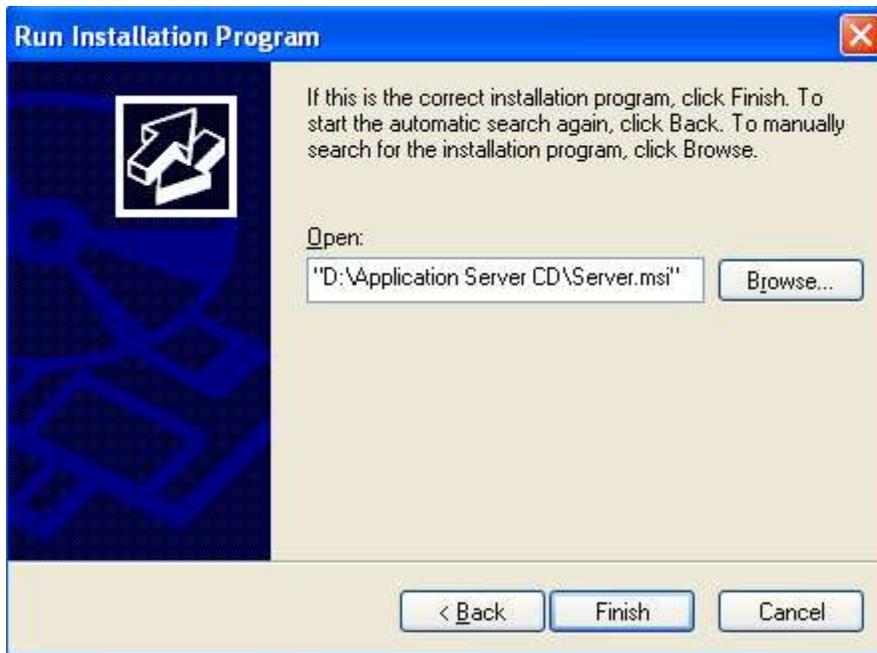
Now click the Browse button



Now find the Application Server folder on the CD and select the Server.msi file and Click Open.



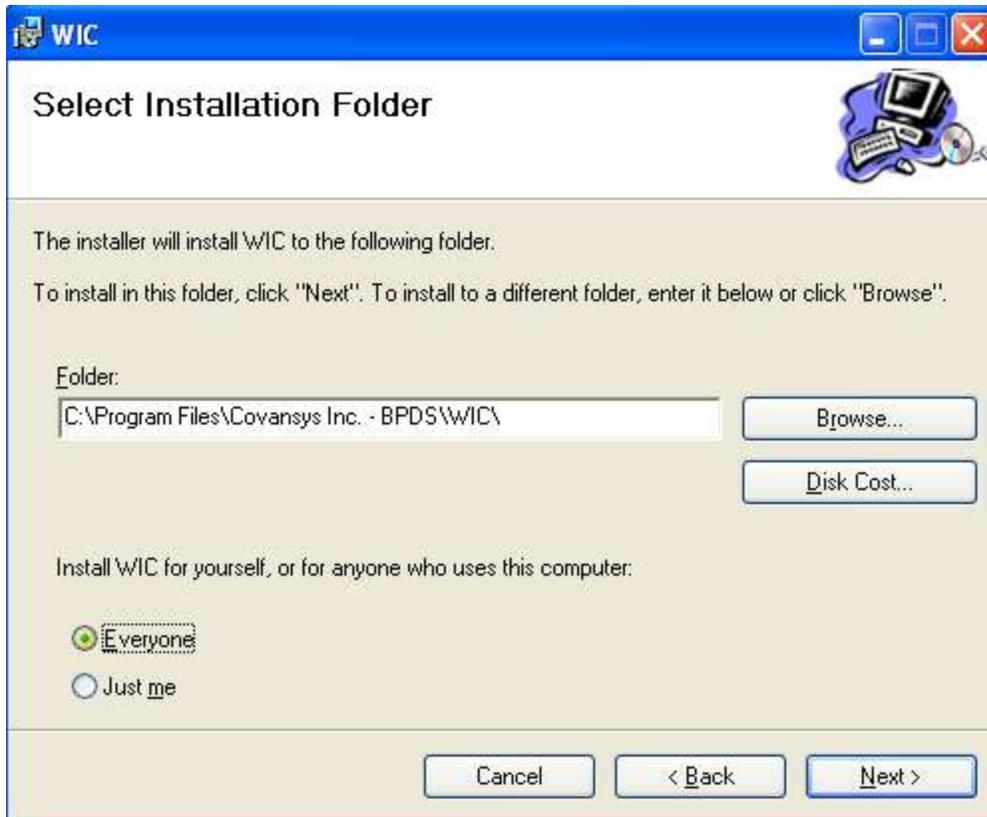
Click Finish



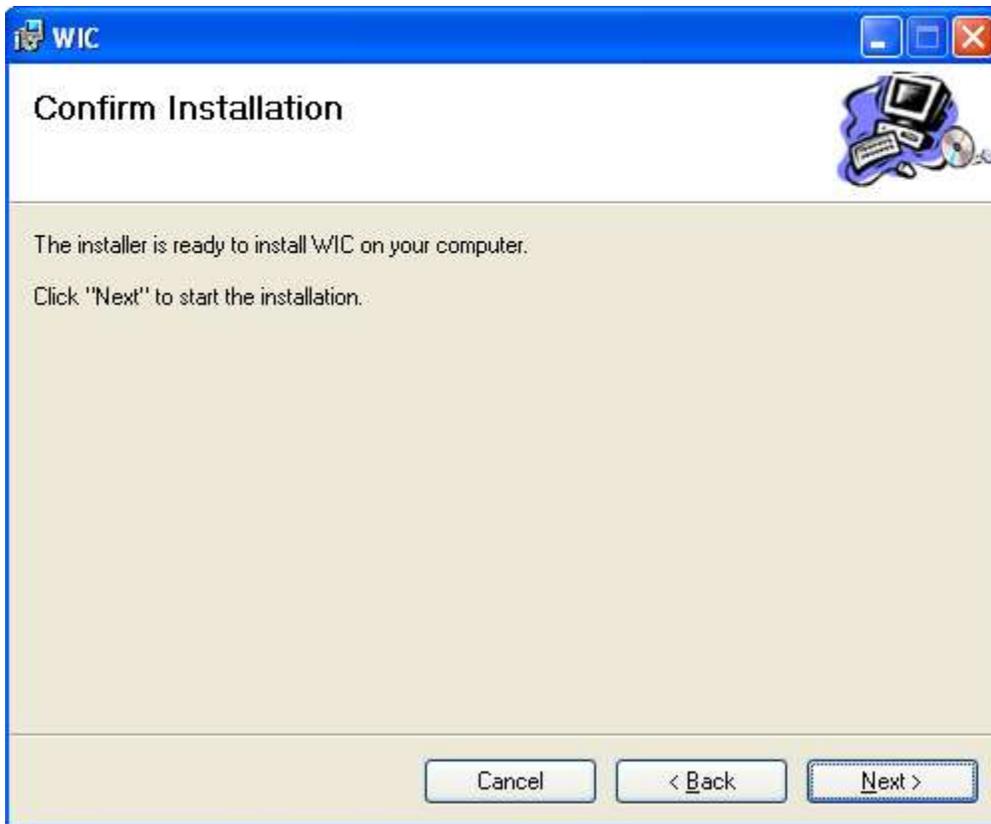
Click Next



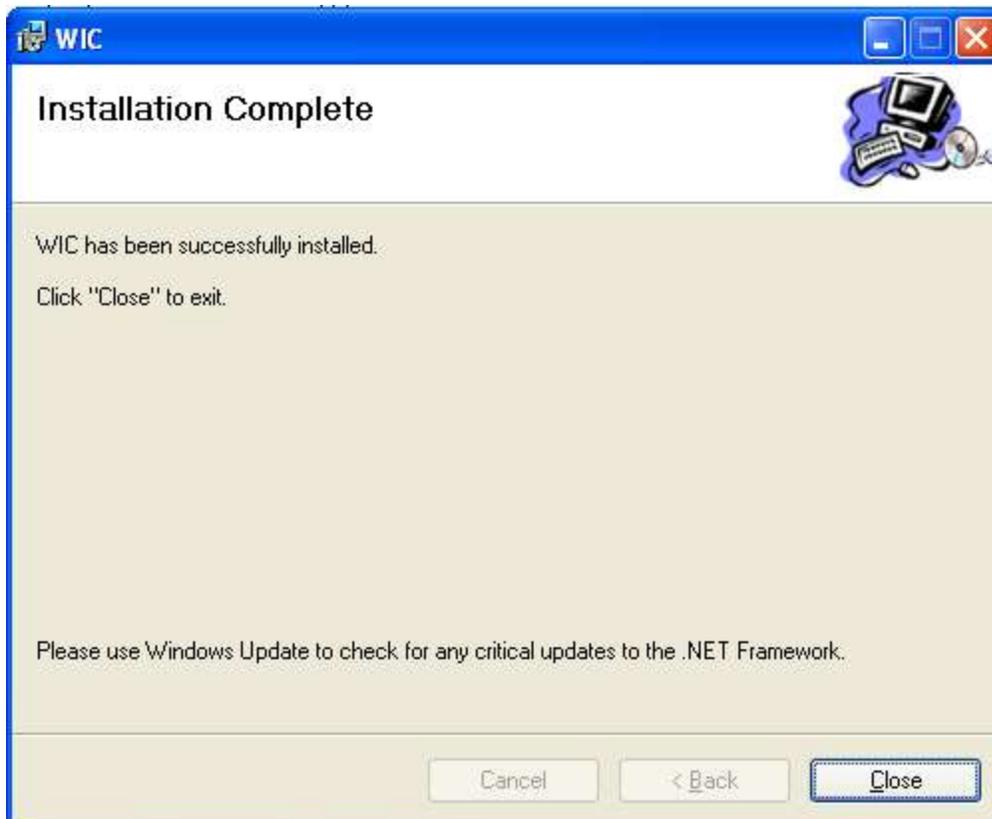
Click the “Everyone” and then click “Next”



Click Next button. This will start the install.



Click Close



Database Updates

After each refreshing the follow SQL needs to be run against the refreshed schema:

```
sp_change_users_login 'update_one', 'spirit', 'spirit'  
go
```

APPENDIX B

Disaster Recovery Plan

Note: The information contained in the Disaster recovery Plan was supplied by Chickasaw Nation Information Technology Helpdesk.

When disaster strikes, whether in the form of a tornado, a blackout, or far more likely common equipment failure, virus attack, or software or user error, your ability to respond well to the crisis can make the difference in how quickly you can resume daily operations. The SPIRIT Disaster Recovery Plan for Computer Equipment is designed to help give you the edge to identify preventive controls for avoiding disasters, to develop strategies for recovery and continued operations, and should work in conjunction with the overall agency disaster recovery plan.

The procedures outlined in this document are intended -

- to ensure computer equipment distributed to the SPIRIT Consortium clinics is secured against theft or damage;
- to ensure malfunctioning or damaged equipment is replaced to support continued clinic operations;
- to ensure virus attacks are identified early to prevent downtime; and
- to ensure software or user error is addressed by the help desk specialist to correct problems effecting clinic operations.

In this document, computer equipment refers to desktop computer systems, laptop computers, uninterrupted power supplies (UPS), MICR printers, laser printers, signature pads, and scanners provided through the SPIRIT Consortium. The procedures outlined in this plan apply to all clinics in the SPIRIT Consortium.

Securing computer equipment:

All agencies in the SPIRIT Consortium are responsible for securing the computer equipment to prevent theft and damage to the equipment. Laptop computers are small and can easily be stolen. The asset loss associated with laptop theft is not the only impact of a theft. Information residing on the computers is confidential and essential for clinic operations. The theft of computer equipment increases the risk that confidential and/or sensitive information will be lost or stolen and used to gain unauthorized access to private networks. Also, the liability concerns increase if confidential information from a third party such as a vendor or customer is lost. Exercising reasonable due diligence in protecting all computer equipment from theft is a necessary part of an acceptable set of security standards.

Approved software:

All computers will have the following approved software loaded on the hard drives.

- Microsoft operating system
- Microsoft Office (Word, Excel, Power Point, Outlook, Access)
- Trend Micro (an anti-virus software)
- Adobe Reader
- SPIRIT application
- Printer drivers for the MICR and laser printers
- Software related to the Signature Pad and Scanner
- Internet Service Provider (ISP) software

In order to maintain the utmost security for client data, agencies must only allow approved software to be installed on the desktop and laptop computers. Computers running unapproved software applications can leave customer data vulnerable to external security breaches. Specifically, any outside messenger programs such as AOL Instant Messenger or file sharing programs such as *Kazaa* or *Limewire* are banned from installation. These programs allow outsiders instant access to items contained on your hard drive. Maintaining standard computer configurations allows the SPIRIT Help Desk to resolve technical software issues in an efficient manner.

Backing up information on the hard drive:

The business interruption losses and administrative costs involved in obtaining and setting up new systems is greatly compounded when employees do not regularly back up the user information on the hard drive. The following paragraphs describe the recommended processes that should be performed on a regular basis to ensure a copy of the information contained on the computers is available and accessible when disasters occur.

Microsoft Office files:

Documents, spreadsheets, databases, Power Point slides, or any files created using Microsoft Office reside on the agency's computer hard drives and are usually located in the "My Documents" folder unless saved to removable media (e.g. CD-R, CD-RW, DVD-R, or USB removable storage media). To ensure availability of these files in the event of a disaster, each agency should periodically make a copy of the files (created using Microsoft Office) to a CD-R, CD-RW or USB removable storage medium (also referred to as flash drive, jump drive, or thumb drive) and store the copy in a secure location. Removable storage media is inexpensive, is small in size, and may prevent future frustrations and costs associated with re-creating Microsoft Office documents in the event of a disaster. The SPIRIT Help Desk is available by phone to assist you with the copy process.

Copying SPIRIT files:

During normal operations, agencies may be using laptop computers in clinic locations that do not have real time Internet access. At the beginning of the day, client database information must be downloaded from the central database server to the laptop computer through an Internet connection to ensure the latest client information is accessible on the laptop computer. At the end of the day, client entries saved to the laptop computer must be uploaded through an Internet connection from the laptop computer to the central database server. This process ensures a copy of the days entries reside on the central database server. The upload/download process is referred to as data synchronizing the client (or data sync client). In the event of a disaster where Internet connectivity is unavailable, the daily operation entries saved on the laptop computer should be copied to a USB removable storage medium to ensure data is not lost if the laptop computer malfunctions or is damaged before data synchronizing with the central database server. The SPIRIT Help Desk is available by phone to assist you with the copy process.

SPIRIT agency backup laptop computer:

Internet service provider connectivity problems may prevent an agency from connecting to the central database server. To circumvent the resulting down time related to this type of disaster, a laptop computer (referred to as the backup laptop computer) has been provided to each agency for backup purposes only. At the beginning and end of each normal operating day, agencies should data sync client information on the backup laptop computer. Following these procedures will ensure agencies have a copy of the latest client information available on the backup laptop computer in case of a disaster. The backup laptop computer should be secure and stored at a different location from the agency's main computer in case of fire, tornado, flood, etc. The battery on the backup computer must be charged and monitored in case of an electrical outage. If you experience a disaster, contact the SPIRIT Help Desk for recommendations and assistance.

Central server notifications:

If a problem arises with the central servers where the servers are not able to send or receive agency information, the SPIRIT Help Desk staff will contact agencies via email or telephone providing estimates of time required to remedy the problem and recommendations regarding backup of agency information. Once the servers are back on-line, the SPIRIT Help Desk will notify agencies by email or phone that servers are able to receive and send agency information.

Virus protection:

Virus detection and protection software is installed on all SPIRIT computers. Agencies are responsible for the annual renewal of the virus protection subscription. Agency computers are configured to download virus protection software updates automatically when connected to the Internet. Should you receive any prompts regarding these updates, choose the default and proceed. If you suspect that the computer has a virus, contact the SPIRIT Help Desk immediately.

Each agency should have policies that govern email and Internet usage. The following recommendations should be included in agency email and Internet policies.

- Consider business ethics when browsing publicly published websites. Limit website visits to business related sites.
- If you receive an email attachment from someone you do not know, do not open the email attachment. Simply delete the email. If the attachment is a business related attachment, the sender should contact you by phone and let you know you will be receiving the attachment. Do not download anything unrelated to business.
- Messenger programs such as AOL Instant Messenger or file sharing programs such as Kazaa or Limewire allow outsiders instant access to items contained on your hard drive. Do not install these programs on the computer.

Updates:

Microsoft provides free updates that address known security vulnerabilities. When you connect to the Internet, the updates will be downloaded to the computer. You may receive prompts

indicating that Microsoft downloads are ready for installation. Should you receive any prompts regarding these updates, choose the default and proceed.

From time to time, system or application updates may be provided to SPIRIT agencies through the SPIRIT Help Desk. The SPIRIT Help Desk staff will contact SPIRIT agencies prior to receiving the updates. The updates may be provided on CD-ROM or through a link to a website. Each agency will receive complete instructions regarding installation procedures. The SPIRIT Help Desk is available by phone to assist you with the installation.

User authentication:

To protect unauthorized personnel from accessing WIC files, each end user will need a user ID and password to access the SPIRIT application. The user ID and password should not be forgotten or shared with others. Passwords should contain eight or more digits, combining random upper and lower case letters, numeric, and punctuation characters.

Employees should guard their passwords and not share their passwords or write their passwords on a sticky note in the office or on a piece of paper in a desk drawer. A policy should be established requiring frequent password changes and employing different passwords for access to the computer and specific files and applications.

Replacement of computer equipment:

The SPIRIT Help Desk will be the point of contact to arrange for loaners (spare equipment) to be shipped to agencies in an attempt to avoid breaks in clinic services. The SPIRIT Help Desk will also act as a liaison for warranty repairs to agency equipment and work with agencies to procure computer equipment in the event of cyclical replacements. All computer equipment questions should be directed to the SPIRIT Help Desk.

Disaster Recovery Plan revisions:

The SPIRIT Disaster Recovery Plan for Computer Equipment is subject to periodic revisions. The tracked revisions will be provided to SPIRIT agencies when updated.

APPENDIX C

Glossary of Terms

ADMINISTRATOR

For Windows XP Professional, a person responsible for setting up and managing domain controllers or local computers and their user and group accounts, assigning passwords and permissions, and helping users with networking problems. Administrators are members of the Administrators group and have full control over the domain or computer.

For Windows XP Home Edition, a person who can make system-wide changes to the computer, install software, and who has access to all files on the computer. A person with a computer administrator account has full access to other user accounts on the computer.

ALPHANUMERIC

Alphabetic and numeric characteristics (letters and numbers).

APPLICATION

A collection of one or more interrelated data processing operations set up to run on a computer on a routine, periodic basis to satisfy a particular functional need.

APPLICATION SOFTWARE

A computer program or set of programs (system) that perform a specific task (such as word processing).

ASCII

American Standard Code for Information Interchange. Standard digital set used for representing information in microcomputers.

AUTHORIZATION

The process that determines what a user is permitted to do on a computer system or network.

BACKGROUND

The screen background image used on a graphical user interface such as Windows. Any pattern or picture that can be stored as a bitmap (.bmp) file can be set as a screen background.

BACKGROUND PROGRAM

A program that runs while the user is working on another task. The computer's microprocessor assigns fewer resources to background programs than foreground programs.

BACKUP COPY

Duplicate copy of data or information stored separately in case of loss or damage to the original.

BOOT

The process of starting or resetting a computer. When first turned on (cold boot) or reset (warm boot), the computer runs the software that loads and starts the computer's operating system, which prepares it for use.

BROWSER

Software that interprets the markup of files in HTML, formats them into Web pages, and displays them to the end user. Some browsers also permit end users to send and receive e-mail, read newsgroups, and play sound or video files embedded in Web documents.

CD

A disk drive that stores and reads data from a compact disk.

CD-R

Recordable compact disc. Data can be copied to the CD on more than one occasion; however, data cannot be erased from the CD.

CD-RW

Rewritable compact disc. Data can be copied to the CD on more than one occasion and can be erased.

CHARACTER MODE

A display mode in which the monitor can display letters, numbers, and other text characters, but no graphical images or character formatting (italics, superscript, and so on).

CLIENT

Any computer or program connecting to, or requesting the services of, another computer or program. Client can also refer to the software that enables the computer or program to establish the connection.

For a local area network (LAN) or the Internet, a computer that uses shared network resources provided by another computer (called a server).

CLIENT APPLICATION

A Windows-based application that can display and store linked or embedded objects. For distributed applications, the application that imitates a request to a server application.

COMPUTER ACCOUNT

An account that is created by a domain administrator and uniquely identifies the computer on the domain. The Windows computer account matches the name of the computer joining the domain.

COMPUTER ADMINISTRATOR

A user who manages a computer. The computer administrator makes system-wide changes to the computer, including installing programs and accessing all files on the computer, and can create, change and delete the accounts of other users.

CONNECT

To assign a drive letter, port, or computer name to a shared resource so that you can use it.

CPU

Central Processing Unit. Main unit within a computer system that contains the circuits that interpret and control the execution of instructions. Directs control of information and computing.

CRASH

Hardware or software failure that renders the computer inoperative.

DAILY BACKUP

A backup that copies all selected files that have been modified the day the daily backup is performed. The backed-up files are not marked as having been backed up (in other words, the archive attribute is not cleared).

DATA

Information that a computer processes.

DATABASE

Compilation of data records in an organized format.

DBMS

Data Base Management System. Software that manages, manipulates, and retrieves data in a database.

DEBUGGING

Process of correcting errors in a program.

DEVICE

Any piece of equipment that can be attached to a network or computer; for example, a computer, printer, joystick, adapter, or modem card, or any other peripheral equipment. Devices normally require a device driver to function with Windows.

DISK

Circular magnetic storage device which is rotated while in use. Also called a "floppy disk, hard disk or compact disk."

DISKETTE

Alternate name for 5-1/4 disks.

DISPLAY

Output device for viewing stored information.

DOCUMENT

Any self-contained piece of work created with an application program and, if saved on disk, given a unique file name by which it can be retrieved.

DOMAIN

A group of computers that are part of a network and share a common directory database. A domain is administered as a unit with common rules and procedures. Each domain has a unique name.

An Active Directory domain is a collection of computers defined by the administrator of a Windows network. These computers share a common directory database, security policies, and security relationships with other domains. An Active Directory domain provides access to the centralized user accounts and group accounts maintained by the domain administrator. An Active Directory forest is made up of one or more domains, each of which can span more than one physical location.

A DNS domain is any tree or sub-tree within the DNS namespace. Although the names for DNS domains often correspond to Active Directory domains, DNS domains should not be confused with Active Directory domains.

DOMAIN NAME

The name given by an administrator to a collection of networked computers that share a common directory. Part of the Domain Name System (DNS) naming structure, domain names consist of a sequence of name labels separated by periods.

DRIVE

An area of storage that is formatted with a file system and has a drive letter. The storage can be a floppy disk, a CD, a hard disk, or another type of disk. You can view the contents of a drive by clicking its icon in Windows Explorer or My Computer.

DRIVE LETTER

The naming convention for disk drives on IBM and compatible computers. Drives are named by letter, beginning with A, followed by a colon.

FILE

One or more items of similar data uniquely identified. A collection of records.

FILE TYPE

In the Windows environment, a designation of the operational or structural characteristics of a file. The file type identifies the program, such as Microsoft Word, that is used to open the file. File types are associated with a file name extension. For example, files that have the .txt or .log extension are of the Text Document type and can be opened using any text editor.

FIRMWARE

Program stored in a computer's memory or Read Only Memory.

FONT

A graphic design applied to a collection of numbers, symbols, and characters. A font describes a certain typeface, along with other qualities such as size, spacing, and pitch.

GROUP

A subset of the network established by the network administrator, usually based on departmental organization or physical proximity in the network. File protection facilities allow read/write restrictions for files and folders for groups, users, and the entire network.

HARD COPY

Computer output printed on paper.

HARD DISK

Disk made of rigid material.

HARDWARE

Physical parts of the computer system.

HIGH RESOLUTION

Quality of a display system or printer capable of reproducing images of great detail accurately.

INITIALIZE

To reset a computer system to a beginning point before starting a task. Also used to format a blank disk.

INPUT/OUTPUT

The transfer of information between a user and/ and or peripheral devices, files and the CPU.

INTERFACE

Device or program that allows separate parts of a computer to work together.

INSTRUCTION

Single order or command within a program.

I/O

See Input/Output.

LIBRARY

Collection of programs or data files.

LOG OFF

To sign off of the network.

LOG ON

To sign on to the network.

MEMORY

Part of a computer CPU that is able to retain binary coded information and instructions.

MENU

Program function options or choices displayed for user selection.

MICROPROCESSOR

CPU of a microcomputer.

MODEM

MOdulator-DEModulator. Peripheral used to interface a digital device with a telephone line, while encoding and decoding sequential bits of information into tone variations. Used for transmitting and receiving data.

NETWORK

Provides the capability for a number of computer systems and devices that are logically linked together to share resources by communicating with each other via telecommunications.

NETWORK ADMINISTRATOR

The person charged with planning, designing, and maintaining the network operation.

NODE

A computer or other device that is a member of the network.

ONLINE

Being connected to a computer system via telecommunications.

OPERATING SOFTWARE

Software program for an operating system.

OPERATING SYSTEM

Program that controls the execution of other programs, or software, within a computer system, and interprets application software commands.

OWNER

The person who "owns" a file. You are the owner of files you create.

PERIPHERAL

Accessory part of a computer system not essential to its operation.

PORT

Connecting point for joining hardware and peripherals to computer system.

POWER SURGE EQUIPMENT

Device that protects computer systems from power fluctuations, which may cause errors or a crash.

PROGRAM

Sequence of specified instructions that tells the computer what to do.

RAM

Random Access Memory. Temporary memory on chips, disk, or similar device. Data is used by the CPU and may be altered by the user. Information in a RAM chip is lost when power to the computer system is turned off.

READ/WRITE MEMORY

Alternate name for RAM.

ROM

Read Only Memory. Permanent memory included in a CPU that cannot be altered by a user or a program. Data in this memory is used by the CPU as soon as power is supplied to the computer system, in order to allow the system to be booted.

SCROLLING

Moving the information displayed on a screen up or down by one or more lines.

SOFTWARE

Computer programs; generally input on disk to a computer system.

USER-FRIENDLY

Capable of use by non-programming, or "user," personnel.

USERNAME

The name of the user that is typed to log on to the network.

WORK STATION

A stand-alone microcomputer or a terminal or microcomputer attached to a host computer.

General Keyboard Shortcuts

Press

CTRL+C

CTRL+X

CTRL+V

CTRL+Z

DELETE

SHIFT+DELETE

CTRL while dragging an item

CTRL+SHIFT while dragging an item

F2

CTRL+RIGHT ARROW

CTRL+LEFT ARROW

CTRL+DOWN ARROW

CTRL+UP ARROW

CTRL+SHIFT with any of the arrow keys

SHIFT with any of the arrow keys

CTRL+A

F3

ALT+ENTER

ALT+F4

ALT+Enter

ALT+SPACEBAR

CTRL+F4

ALT+TAB

ALT+ESC

F6

F4

SHIFT+F10

ALT+SPACEBAR

CTRL+ESC

ALT+Underlined letter in a menu

To

Copy.

Cut.

Paste.

Undo.

Delete.

Delete selected item permanently without placing the item in the Recycle Bin.

Copy selected item.

Create shortcut to selected item.

Rename selected item.

Move the insertion point to the beginning of the next word.

Move the insertion point to the beginning of the previous word.

Move the insertion point to the beginning of the next paragraph.

Move the insertion point to the beginning of the previous paragraph.

Highlight a block of text.

Select more than one item in a window or on the desktop, or select text within a document.

Select all.

Search for a file or folder.

View properties for the selected item.

Close the active item, or quit the active program.

Displays the properties of the selected object.

Opens the shortcut menu for the active window.

Close the active document in programs that allow you to have multiple documents open simultaneously.

Switch between open items.

Cycle through items in the order they were opened.

Cycle through screen elements in a window or on the desktop.

Display the Address bar list in My Computer or Windows Explorer.

Display the shortcut menu for the selected item.

Display the System menu for the active window.

Display the **Start** menu.

Display the corresponding menu.

name

Underlined letter in a command
name on an open menu

F10

RIGHT ARROW

LEFT ARROW

F5

BACKSPACE

ESC

SHIFT when you insert a CD into
the CD-ROM drive

Carry out the corresponding command.

Activate the menu bar in the active program.

Open the next menu to the right, or open a submenu.

Open the next menu to the left, or close a submenu.

Refresh the active window.

View the folder one level up in My Computer or Windows
Explorer.

Cancel the current task.

Prevent the CD from automatically playing.

APPENDIX D

End of Month (System Administration)

The following information is provided for System Administration purposes with the End of Month processes.

Daily Maintenance Procedures

1. System Administrator - Review End of Day logs each day through the Schedule Job Administration application. The system administrator or personnel responsible for monitoring end of day will invoke the Schedule Job Administration Application and view the End of Day logs for potential errors that may need to be resolved before End of Day can process for the following day. In rare circumstances where End of Day is ended by user interaction or power surge
2. WIC Banking – You can access the <https://dataimagegateway.com> web site for SPIRIT information. The system administrator responsible for bank transactions can access this site and view the bank transactions daily. Username and Password are required.

Monthly

Month End consists of two primary components: 1) Desktop Scheduling and 2) Month End Processing.

Desktop Scheduling

Scheduled Job Administration

Month End is scheduled using the Scheduled Jobs Administration interface.



Figure 1 – Scheduled Job Administration Main Window

To invoke WIC Month End Administration, click on the Scheduled Jobs option, WIC Month End Administration and select Run.

WIC Month End Administration

The WIC Month End Administration interface provides for adding and removing Month End from the schedule and the options to view or purge the Month End log. Also displayed are the latest

Month End settings. The Month End Settings are helpful in understanding the system issued messages when attempting to add or remove from the schedule. For example, if the last status shows errors, then the user can expect to be guided by the system via messages when they select Add to Schedule. The messages will give options for restarting based on Month End settings and data.

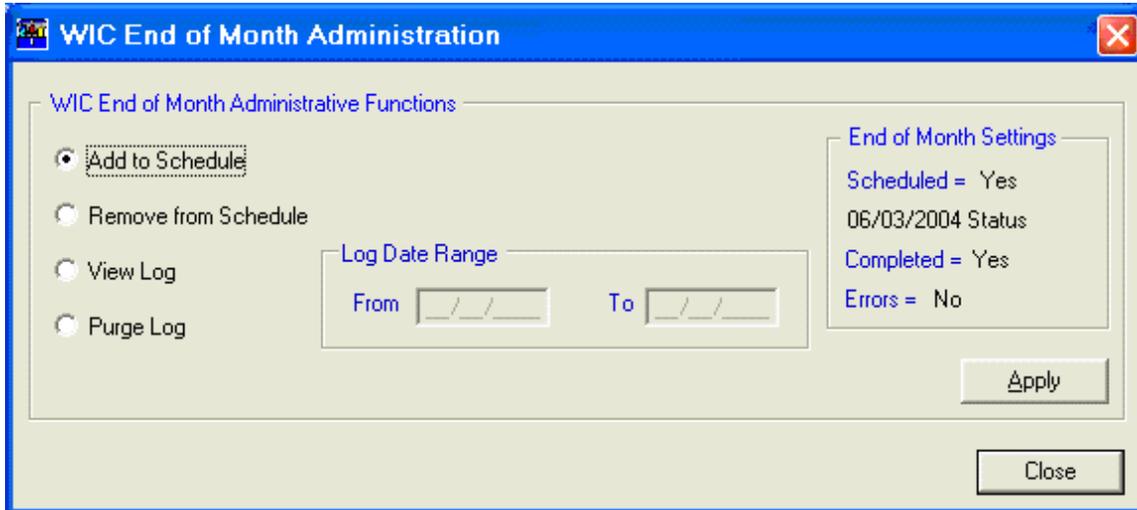


Figure 2 - WIC Month End Administration Main Window

Add to Schedule

To schedule Month End, select option Add to Schedule. Upon selection of Add to Schedule, pre-schedule validation occurs that involves:

1. Confirmation that Month End is currently not executing. If it is currently running, a message will be issued.
2. Verifies Bank Reconciliation totals. A state business rule is used to determine if this process is applicable to the state. If it is applicable and the bank totals do not reconcile, a text file is displayed with the bank totals. Month End cannot be scheduled until they have been corrected.
3. Determines the state/status of Month End. Each state/status is described below.

Month End State / Status

1. Normal Schedule:

The previous Month End executed successfully and the current month is ready to process. If the Month End status is determined to be a normal schedule, the following window will be displayed for confirmation to continue.

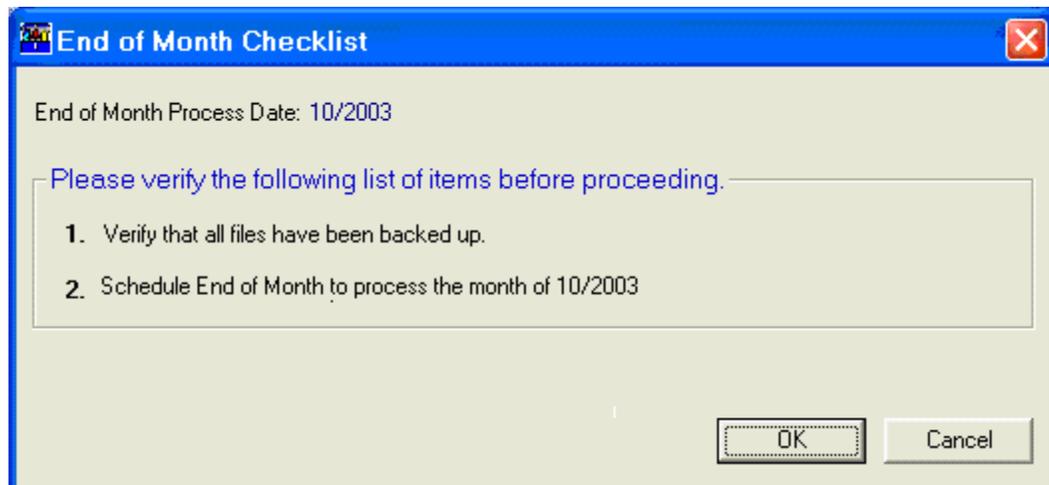


Figure 3 – Month End Checklist

Upon selection of OK, Month End will be scheduled to run.

- ◆ The exact time is dependent on when the daily schedule begins. If Month End is scheduled prior to when the daily schedule begins, then it will run on the days schedule; otherwise, it will run on the next day's schedule.
- ◆ The Month End Settings will be changed to show Scheduled = Yes.

Restart Mode:

The current month end completed with errors. The Month End Settings, Errors = Yes, is indication that the state of Month End is restart mode. The Month End administrator would have received email notification from the Scheduled Job utility named Interrogator, that there was an error while processing Month End.

All errors will need to be researched and analyzed by technical support before attempting to add to Schedule. To assist in the understanding of the error, review the log to determine which processes completed successfully and those that completed with errors.

There are two types of restart a) Required Process Restart and b) Optional Process Restart.

Restart Type - Required Process

A required process did not complete successfully. The current month end must be restarted and allowed to complete all required processes. No additional Month End processing is allowed until this situation is resolved. It is recommended that you view the log prior to proceeding to determine which processes are affected by the restart.

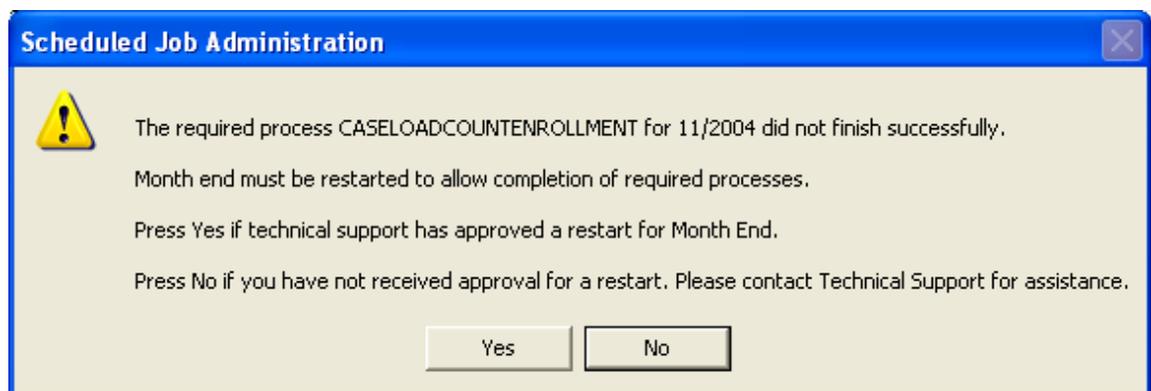


Figure 4 – Required Process Restart Message

Press Yes if technical support has given approval to proceed.

- ◆ Figure 3, Month End Checklist, will display for user confirmation. When confirmed, Month End will be scheduled to restart beginning with the process displayed.
- ◆ Any processes prior to the displayed process will not be processed again since they have successfully completed. Any process that follows the displayed process will run once the restarted process has completed successfully.
- ◆ If the restart is scheduled prior to when the daily schedule begins, then it will run on the days schedule; otherwise, it will run on the next day's schedule.
- ◆ The Month End Settings will be changed to show Scheduled = Yes.

Press No if you are unsure that the issues have been resolved and want to cancel the restart.

Restart Type – Optional Process

An optional process did not complete successfully. When an error occurs with an optional process, all processes that follow the displayed process are allowed to continue. Month End always restarts with the first optional process that failed. If more than one optional process failed, they will also be restarted.

It is recommended that the log be viewed before making a decision. The processing order and where the displayed process is sequenced should be considered before restarting. For example, if the displayed process was the first optional process and the only process to fail, then it may be preferable to run the displayed process on demand rather than restarting Month End. Restarting will rerun the displayed process and all processes that follow in the processing order.

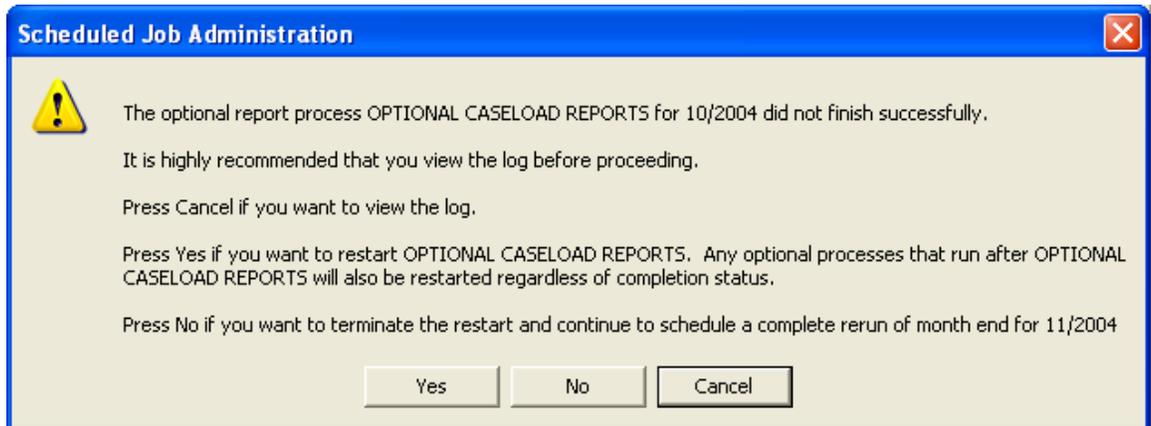


Figure 5 – Optional Process Restart Message

Press Yes to schedule Month End restart beginning at the displayed optional process going forward.

- ◆ Figure 3, Month End Checklist, will display for user confirmation.
- ◆ If the restart is scheduled prior to when the daily schedule begins, then it will run on the days schedule; otherwise, it will run on the next day's schedule.
- ◆ A restart for an optional process is only applicable for the current month. If the restart is delayed until the next month end processing, the above message will not be displayed and a normal month end will be scheduled as described above for Normal Schedule. The optional processes will need to be run on demand if this situation occurs.

Press No to ignore the restart and to schedule a complete rerun of Month End for the current month.

- ◆ Figure 3, Month End Checklist, will display for user confirmation.
- ◆ If the rerun is scheduled prior to when the daily schedule begins, then it will run on the days schedule; otherwise, it will run on the next day's schedule.
- ◆ Figure 6, Rerun Current Month End, will display for user confirmation to rerun.

Press Cancel for no action at this time.

Remove from Schedule

To remove Month End from the schedule, select option Remove from Schedule as shown on Figure 2 - WIC Month End Administration Main Window. Upon selection of Remove from Schedule, the system will verify that Month End is not currently running. If it is not running, then Month End will be removed from the schedule.

Month End is removed automatically from the schedule each time it runs with or without errors. The Month End Settings will generally show Scheduled = No. Use this option if you Add to Schedule and then must remove from the schedule before Month End actually runs.

Note: If the Month End scheduled was a restart or rerun, Remove from Schedule will reset Month End settings to the original values. The restart or rerun must be rescheduled by selecting Add to Schedule. The restart or rerun messages, whichever is applicable, will display again.

View Log

To view the Month End Log, select option View Log as shown on Figure 2 - WIC Month End Administration Main Window. A "From Date" and "To Date" range is required.

The Month End process that runs on the server logs an entry prior to each process. When possible, error messages are also logged. The Add to Schedule and the Remove from Schedule also writes entries to this log.

Purge Log

To purge the Month End Log, select option Purge Log as shown on Figure 2 - WIC Month End Administration Main Window. A "From Date" and "To Date" range is required.

It is recommended that you periodically purge data from the Month End log.

Month End Processing

The main processing for Month End was designed to run on a server. The application interface does not require interaction from a user. However, there are two exceptions that will require acknowledgement. 1) If the application is started again while it is currently running a message will be issued stating that another instance of the application is already running. 2) If the database table Currently_Executing shows a process that is in conflict with Month End a message will be displayed. The message will display the process name that conflicts with Month End.

The Month End administrator controls when Month End will execute using Desktop Scheduling as described in Section 1 of this document. When the administrator adds Month End to the schedule, the database table Scheduled_Job_Control is updated indicating that Month End is scheduled. This does not actually invoke Month End to run. Month End must be on an automated scheduler or manually invoked. When invoked, Month End reads Scheduled_Job_Control as the first step before proceeding. If the table indicates scheduled, then processing continues; otherwise, Month End immediately terminates successfully. This feature provides for the flexibility of keeping Month End on an automated scheduler to run each day without the need to alter the schedule. It is the Scheduled_Job_Control table maintained by the Month End administrator that determines when the processing actually takes place for the month.

Month End is automatically removed from the schedule by the Scheduled Job utility, Interrogator. It is always removed regardless if it completed successfully or completed with errors. Interrogator notifies the Month End administrator via email of the completion status.

If there are errors, the Month End administrator will need to work with technical support to correct the data before attempting to add month end to the schedule. In all cases, normal schedule, rerun and restart, the Month End administrator must use WIC Month End Administration, Add to Schedule to schedule Month End.

The Month End processing consists of required and optional processes. State business rules control which processes are applicable to the state. Only the processes applicable to the state will be executed.

The End of Month Processing includes:

1. Rolling the Process Control Table Dates

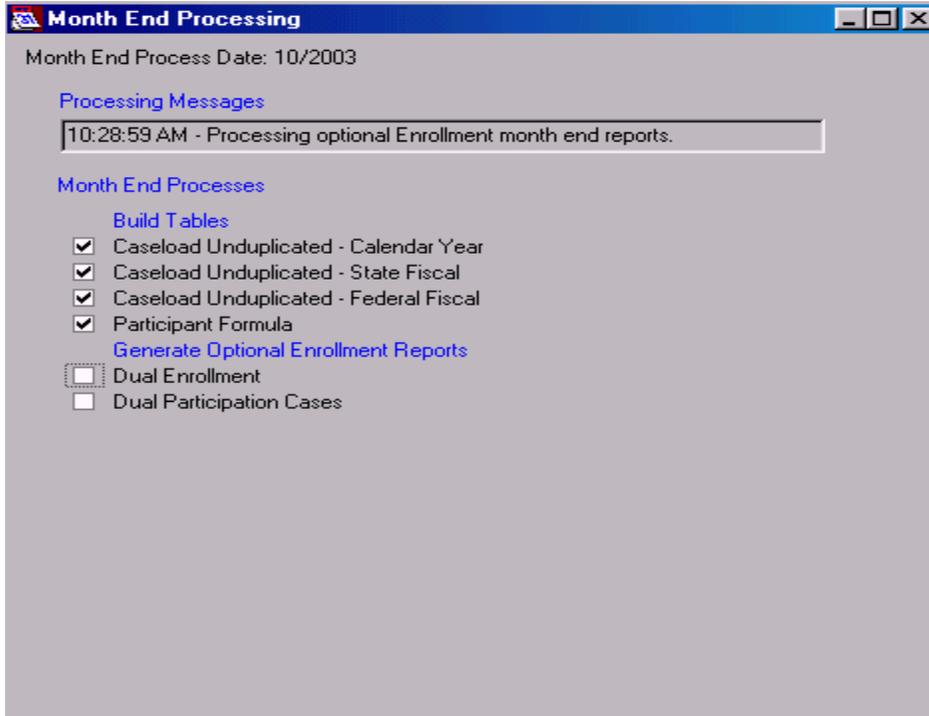
2. Build Tables
 - Reported Participation Data
 - Enrollment Participation Data
 - Rebate Items
 - Vendor High Risk
 - Caseload Unduplicated - Calendar Year
 - Caseload Unduplicated - State Fiscal
 - Caseload Unduplicated - Federal Fiscal
 - Dual Enrollment - Enrolled and Participation
 - Participant Formula
 - Caseload Management Projection
 - FI Redemption Reconciliation
3. Generate Financial Reports
 - WIC Food Obligations and Expenditures
 - Average Cost Per Food Instrument Type
 - Food Instrument Redemption Summary
 - Food Instruments Redeemed Early
 - Food Instruments Redeemed Late
 - Supplier Rebate
 - Obligation Value for Outstanding FIs Issued
 - FMNP Food Expenditures
4. Generate High Risk Reports
 - Food Instruments Redeemed within \$5.00 of the Maximum Allowed Report
 - Food Instruments Redeemed within 85% of the Maximum Allowed Report
 - Vendors Whose Food Average Package Cost is More Than 10% Above Peer Group Average Report
 - Percent of Increase in Food Instruments Over Previous Month's Redemptions Report
5. Create Files
 - Create CDC Pregnancy File
 - Create CDC Pediatric File
 - Create External Dual Participation File for Oklahoma
6. Generate Optional Caseload Reports
 - Redeemed Participation Monthly
 - Reported Participation Monthly
 - Reported Participant High-Risk Outreach
 - Redeemed Food Instruments/Expenditures
 - Participation Processing Statistics
 - Enrollment Monthly
 - Unduplicated Enrollment-Yearly (Calendar Year)
 - Unduplicated Enrollment-Yearly (State Fiscal Year)
 - Unduplicated Enrollment-Yearly (Federal Fiscal Year)
 - Enrollment Unduplicated – Yearly
 - Reported Participation Unduplicated – Yearly
 - Redeemed Participation Unduplicated – Yearly
 - Redeemed Participation Priority Summary

- Redeemed Participation High Risk Priority Goal
 - Estimated Eligible Comparison Reported Participation
 - Enrollees by Age and Race/Ethnicity
 - Caseload Management Projection System Report
 - Food Instrument Package Cost
7. Generate Optional Nutrition Reports
 - Formula Compliance
 8. Generate Optional Enrollment Reports
 - Dual Enrollment
 - Dual Participation Cases
 9. Generate Optional Food Instrument Reports
 - List of Items Paid Without Issuance
 - Voided/Stolen and Cashed Exceptions
 10. Generate Optional Operation Reports
 - Migrant Enrollment
 - Non-Participation Reason by Category
 - Formula Supplementation of Breastfed Infants
 - Breastfeeding Certification Periods
 - Food Prescriptions
 - Special Formula
 - Participant Insurance Type
 - Medicaid Adjunctive Eligibility
 11. Generate Optional Financial Reports
 - Food Instruments Rejected for Payment
 12. Generate Optional Vendor Reports
 - High Cost Vendor Summary by Food Instrument Type
 - High Cost Vendor Summary by Vendor
 - High Cost Food Instrument Report
 - Low Variance Vendor Summary
 - Large Number of FI Rdmd Outside of Area
 - Redemption Twenty Percent Change
 - Small Volume Vendors < Than 25 Participants per Month
 13. Log Progress to the End of Month Log File

The following is a list of the required processes available in End of Month. As noted, there is a state business rule for each process so all processes may not be applicable to the state. The names shown below are used in user display messages and log messages.

CASELOAD COUNT
 CASELOAD ENROLLMENT
 CASELOAD REBATEITEMS
 VENDOR HIGHRISK DATA
 CASELOAD COUNT UNDUP
 DUAL ENROLLMENT
 PARTICIPANT FORMULA
 REDEMPTION RECONCILIATION
 CASELOAD PROJECTION
 CDC FILES

EXTERNAL DUAL PARTICIPATION FILE
FINANCIAL REPORTS
HIGH RISK REPORTS



The following is a list of the optional processes available in End of Month. As noted, there is a state business rule for each process so all processes may not be applicable for your state. The names shown below are used in user display messages and log messages.

OPTIONAL CASELOAD REPORTS
OPTIONAL NUTRITION REPORTS
OPTIONAL ENROLLMENT REPORTS
OPTIONAL FOOD INSTRUMENT REPORTS
OPTIONAL OPERATION REPORTS
OPTIONAL FINANCIAL REPORTS
OPTIONAL VENDOR REPORTS

APPENDIX E

End of Day (System Administration)

The following information will discuss the functions of the End of Day Process application that is run either manually or automatically on the Server at the end of the business day. The main processing for End of Day is designed to run on a server. The application interface does not require interaction from a user.

However, there are two exceptions that will require acknowledgement.

- 1) If the application is started again while it is currently running a message will be issued stating that another instance of the application is already running.
- 2) If the database table Currently_Executing shows a process that is in conflict with End of Day a message will be displayed. The message will display the process name that conflicts with End of Day.

For example, the End of Month processes use bank paid/rejected information for food instruments, which End of Day processes. Therefore the two processes must not run simultaneously.

The End of Day administrator controls when End of Day will execute using Schedule Job Administration (Chapter 09) and Windows Task Scheduler. When the administrator adds End of Day to the schedule, the database table Scheduled_Job_Control is updated indicating that End of Day is scheduled. This does not actually invoke End of Day to run. End of Day must be scheduled through Window Task Scheduler or some other form of automated scheduler or manually invoked. When invoked, End of Day reads Scheduled_Job_Control as the first step before proceeding. If the table indicates scheduled, then processing continues; otherwise, End of Day immediately terminates successfully. This feature provides for the flexibility of keeping End of Day on an automated scheduler to run each day without the need to alter the schedule. It is the Scheduled_Job_Control table maintained by the End of Day administrator that determines when the processing actually takes place for the month.

The End of Day Dialog will be initially displayed in a minimized state. The End of Day window can be restored by double clicking the title bar. A progress bar is displayed while the processes are running. All informative and error condition messages are saved to the End of Day event log. The processes run during End of Day are determined by the values that are set for each State Business Rule.

Log On

When End of Day Process is started, it will log into the system using a known username and password. This will give the program access to the database tables it needs to get the required information. The user name and password will come out of the registry from the server where End of Day is run:

```
HKEY_LOCAL_MACHINE\SOFTWARE\PDA\<STATE>VENDOR\COMMON\OBJECTOWNER.
```

The service name will be taken out of the registry on the server where End of Day is run:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ PDA  
\<STATE>VENDOR\COMMON\SQLSERVERDBSERVICENAME.
```

Response File

Upon selection of the End of Day Process, the system will check for a Response File on the server where End of Day is run. The End of Day Process will not continue if the response file is missing or sends an unsuccessful message back to the system.

If applicable for your State, End of Day will look for Response file on the server where End of Day is run in the \<StateCode>EOD\CSFPISSUANCE\RESPONSE and CSFPSTOPPAY\RESPONSE folder.

If applicable for your State, End of Day will look for Response file on the server where End of Day is run in the EOD\FOODINSTRUMENT\REPOSE folder.

Progress Meter

When the End of Day dialog is restored (not minimized), the progress meter is displayed to inform the user of End of Day processing status. The progress meter displays the percentage complete for the processing of the files. Once the meter reaches 100% the End of Day process is complete.

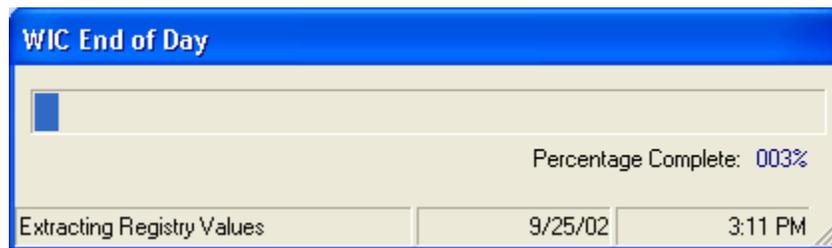


Figure 1– End of Day Dialog

Controls

End of Day Percent Complete Progress Bar

This control displays a progress indicator for the End of Day process.

Characteristics

The progress bar will be enabled when the form is active. It will display, in a graphical display, the percentage of completion.

Validation of Required Settings Logged messages

This section describes the processes (navigation) that take place as a result of the actions taken on the End of Day Conflicts.

System Registry Entries

If the system registry has been updated or corrupted, a system message is written to the log file with the message text, "The system was unable to retrieve the end of month reports file folder name from the registry. Please contact technical support for assistance."

If the required registry entry for End of Day is not found in the Windows System Registry, End of Day Processing will be terminated. A message box will be written to the log file with the message text "A directory or file defined in the Registry for the End of Day process does not exist".

Order of processing

The order of processing end of day will be determined by the value in the State Business Rules entity and if applicable for your state. Processes, imports and exports applicable for your state will be processed. Processes are run first, imports second, and exports last.

Process Sanction Points

Sanction points that no longer apply will be 'rolled-off' the system. The sanction points accumulate over the lifetime of the Vendor contract. These sanction points may no longer be counted against a vendor after a period of time. Each violation has a different expiration date that varies from 0 days to infinite. The End of Day Process will roll-off the expired sanction points that meet certain criteria. This process is applicable for your state if the State Business Rule EOD_PROCESSSANCTIONPOINTS = 'Y'.

Roll-off points

If EOD_PROCESSSANCTIONPOINTS = 'Y' in the StateBusiness rules table, all Sanction points in the Violation table with an ApplyUpTo date greater than the EODLastRunDate in the System Information table and less than or equal to the current system date will be gathered and subtracted from the parent records in the in the FollowUpActivity table and the Event table.

Process Pending Disqualification

The End of Day process will change a vendor to a Disqualified status if the vendor grace period has expired and the vendor is in a Pending Disqualification status. This process is applicable for your state if the State Business Rule EOD_PROCESSPENDINGDISQUALIFICATION = 'Y'.

Process Pending Disqualifications

If EOD_PROCESSPENDINGDISQUALIFICATION = 'Y' and the TerminationDate in the TermDisqualification table is greater than the EODLastRunDate in the SystemInformationtable and less than or equal to the current system date, the system will change the Vendor from a Pending Disqualification status to a Disqualification status. The system will calculate the ReinstatementDate for the vendor. The ReinstatementDate is calculated by adding the DaysDisqualified in the TermDisqualification table to the current system date for the applicable record. If more than one record exists, the most recent record is applied. The calculated date is added to the ReinstatementDate field in the Vendor table for the associated vendor record.

Process 3 Month Rolling Average for Peer Group Pricing

An End of Day process will recalculate the peer group average and maximum prices every 2 weeks based upon actual redemption to obtain a 3-month (12 week) rolling average for the peer group food instrument type or food item. This process is applicable for your state if the State Business Rule EOD_3MONTHROLLINGAVG = 'Y'.

This calculation will not replace the manually calculated Average Price for each food item unless EBT is enabled. The manually calculated average price for each food item is needed for state office obligations, reporting and rebates when paper FIs are issued. It will replace the manually calculated Average and Maximum Prices for the Food Instrument Type and Peer Group.

Process 3 Month Rolling Average

For Paper Food Instruments:

The system will calculate the 3-month rolling average every 2 weeks by selecting issued food instruments that have been redeemed over the last 12 weeks. It will calculate the average redemption amount (the mean) within each food instrument type and vendor peer group combination and update the AvgPrice column in the PEERGROUPOODINSTTYPEPRICE table. For each vendor peer group and food instrument type it will determine the standard deviation value (the mean of the mean) and increase the maximum price by the value set for the EOD_3MONTH_ROLLING_AVG_NBR_STD_DEVIATIONS business rule to determine the standard deviation. This information is stored in the Price column of the PEERGROUPOODINSTTYPEPRICE table.

For EBT:

The system will calculate the 3-month rolling average every 2 weeks by selecting redeemed EBT (electronic benefit transactions) over the last 12 weeks. It will calculate the average redemption amount (the mean) within each food item and vendor peer group combination and update the AvgPrice column in the PEERGROUPOODITEM table. For each vendor peer group and food item it will determine the standard deviation value (the mean of the mean) and increase the maximum price by the value of one standard deviation. This information is stored in the MaxPrice column of the PEERGROUPOODITEM table.

The AvgPrice and Price columns in the PEERGROUPOODINSTTYPEPRICE table will be updated by selecting FI with EBT redemption over the last 12 weeks, summing the peer group food item average price and max price for each food item and its quantity on the FI to set the FI Type average price and price.

Process Reinstate Vendor and Vendor Stamp

The end of day process will reinstate vendors and vendor stamps

Reinstate Vendor and Vendor Stamp

The system will update all vendors, if the Reinsate.ReinstateDate is <= the current system date and the Reinsate.UpdateRecord = 'U'. The end of day process will set the Vendor.CurrentStatus = '3' (enrolled). The system will update the StatusHistory table with the change in vendor status information.

If the ReinstateVendorStamp flag = 'Y', the system will update the VendorStampHistory with the change in stamp information. The system will remove the vendor from the TermDisqualification table. The system will remove the DeactBankEffective date from the TerminateStamp table for the reinstated stamp number for the primary vendor stamp number (Vendor.StampNumber). The system will set the Reinsate.UpdateRecord = 'N' for the VendorID

Adjust/Archive/Purge Process

The End of Day process will change (or move) a participant to Agency '88' when the participant is no longer eligible for WIC. This process is applicable for your state if the State Business Rule EOD_PROCESSADJUSTMENTSHIDES = 'Y'.

Process Adjust Records

If EOD_PROCESSADJUSTMENTSHIDES = 'Y', the system will update Member records to the appropriate status depending on the following criteria.

ADJUST RULES FOR EOD	ACTION
Child records over the Age defined in the State Business Rule. <i>MaximumChildAge</i> and not in a valid certification process.	Change to Categorically Ineligible
Women over the Age defined in the State Business Rule. <i>MaximumWomanAge</i> and not in a valid certification process.	Change to Categorically Ineligible

<p>Participants who have been certified for more for more days than the value of the <i>CertLimitWithPendingIDProof</i> business rule without Proof of ID will be marked as terminated. Homeless participants are excluded from this process.</p> <p>If the participant is an Infant or a Child, this is determined by validating the Member.IdentificationProof value = <i>'PendingIDProofValueChild'</i> business rule and the current system date is greater than the <i>CertLimitWithPendingIDProof</i> business rule and Household.Homeless value is 'N' or null.</p> <p>or</p> <p>If the participant is a Woman, this is determined by validating the Member.IdentificationProof value = <i>'PendingIDProofValueWoman'</i> business rule and the current system date is greater than the <i>CertLimitWithPendingIDProof</i> business rule and Household.Homeless value is 'N' or null.</p>	<p>Mark as terminated</p>
<p>Participants who have been certified for more days than the value of the <i>CertLimitWithPendingResidencyProof</i> business rule without Proof of Residency will be marked as terminated. Homeless participants are excluded from this process</p> <p>For all WIC Categories, this is determined by validating the Member.ResidencyProof value = <i>'PendingResidencyProofValue'</i> business rule and the current system date is greater than the <i>CertLimitWithPendingResidencyProof</i> business rule and Household.Homeless value is 'N' or null.</p>	<p>Mark as terminated</p>
<p>Participants who have been certified with pending proof of income eligibility for more days than the value of the <i>CertLimitWithPendingIncomeProof</i> business rule without additional income information that includes a proof of income.</p> <p>For all WIC Categories, this is determined by validating the IncomeContact.PendingProof value = 'Y' and the current system date is greater than the <i>CertLimitWithPendingIncomeProof</i> business rule.</p>	<p>Mark as terminated</p>
<p>Categorically ineligible participants.</p>	<p>Mark as terminated</p>
<p>Participants who have been certified with delayed blood for more days than the value of the <i>CertLimitWithDelayedBlood</i></p>	<p>Mark as terminated</p>
<p>Participants who have failed to pick up food instruments for two consecutive months or have failed to re-certify for 31 days past their certification due date who are not in a</p>	<p>Mark as terminated</p>

new certification process	
Participants who have been certified with risk factor 503 (Presumptive Eligibility) for more days than the value of the <i>CertLimitWithRF503NoHW</i> business rule without a height/weight measurement contact	Mark as terminated
Participants who have been certified with risk factor 503 (Presumptive Eligibility) for more days than the value of the <i>CertLimitWithRF503NoBlood</i> business rule without a blood work contact	Mark as terminated
Participant who have started a certification attempt but did not complete within the time allowed Adjust Certification Records: <ol style="list-style-type: none"> 1. Participants with a WICSTATUS of Pregnant (P) and a certification has been started but not completed within the number of days defined in the business rule <i>IncompCertLimitPregnant</i> from the certification start date, the participant's certification record is changed to ineligible. 2. Participants whose household record indicates he/she is a Migrant and a certification has been started but not completed within the number of days defined in the <i>IncompCertLimitMigrant</i> business rule from the certification start date, the participant's certification record is changed to ineligible. 3. All Participants with the exception of pregnant women and immigrants, if a certification has been started but not completed within the number of days in the <i>IncompCertLimitOther</i> business rule from the certification start date, the participant's certification record is changed to ineligible. 	Change certification to ineligible and queue Ineligibility notice
Infant to a child when the infant reaches his or her first birthday unless they are currently in a new certification attempt. A pseudo-certification record will be created for the child, and all applicable risk factors will be carried forward from infant to the child pseudo-certification record.	Change WIC Category from I to C
Synchronize the certification information in the Member table to the certification information in the CertContact table when the current certification start date is greater than the certification start date in the Member table.	Update the Member table with the CertContact information.
Update the Valid Certification flag when the participant is no longer in a valid certification	Update Valid Certification flag
Reset all On Premises times for the household members	Reset OnPremisesTime in Member Record

Process Archive Records

The End of Day Process automatically archives records by changing the Agency ID in the Member table to '88'. Agency '88' is used to indicate the member is archived from the active system and will not be visible to the user in the Service Site Application. The member is used for historical reporting, and is not used for current reporting.

ARCHIVE RULES FOR EOD	ACTION
Participants who have not been back for 60 days after applying for WIC	Move to agency '88'
Participant was terminated more than 6 months ago and has not been serviced and they are not currently in a new certification attempt.	Move to agency '88'
Participant whose last certification attempt was ineligible more than 6 months ago and has not been serviced.	Move to agency '88'

Process Purge Records

The End of Day Process automatically archives records by deleting them from the system database.

PURGE RULES FOR EOD	ACTION
Purge Household records that have no members	Delete Household record
Purge Event Logs older than 14 days.	Delete EventLog records
Purge Business Hours Older than 90 days	Call Appointment Scheduler Purge
Purge Appointments at least 3 months old	Call Appointment Scheduler Purge
Purge Class Enrollments older than 7 months	Call Appointment Scheduler Purge
Purge Group Education Classes older than 7 months	Call Appointment Scheduler Purge
Purge Holidays older than 90 days	Call Appointment Scheduler Purge

Send/Receive External Files Process (FTP)

If your state has both Covansys front-end and back-end system the End of Day process will run FTP processes to Send/Receive external files. This process is applicable for your state if the State Business Rule EOD_SENDRECEIVEEXTERNALFILES = 'Y'. Refer to Chapter 07 - Send_Receive (FTP or Dialup) (EOD).doc for more information on this process.

Import Files

Files created for import to the COVANSYS system are placed in the required directories by the COVANSYS system, an external system or the user. Some files are received for the sole purpose of exchanging data with systems that do not have the COVANSYS front-end applications. The function of moving, copying, backing up and archiving all import files is a manual function performed by the user. The COVANSYS system will then import all files according to the State Business Rules. The registry key for the import file directory is
 HKEY_LOCAL_MACHINE\SOFTWARE\PDA\
 <STATE>VENDOR\VendorEOD\ReceiveFromDirectory

Import Issuance File Process

The End of Day process will import Food Instrument Issuance data from an ASCII file format. This process is applicable for your state if the State Business Rule EOD_ISSUANCEFILEIMPORT = 'Y'.

Process Issuance File

If EOD_ISSUANCEFILEIMPORT = 'Y' and an Issuance file is located in the \\<STATECODE>EOD\ISSUANCE\ directory, the End of Day Process will Add/Update the Issuance data in the associated Food Instrument tables. Refer to Chapter 05 – Banking Files (ASCII) (EOD).doc for specifics on the ASCII file layout. If an import file is found then it will be processed, if not the process is bypassed. If multiple import files are found for a process then the import files will be processed in order from oldest to newest based on import file date and time stamp. Import files are renamed after processing so they will not be processed more than once.

Import Banking Paid File

The End of Day process will import Banking Paid data from an ASCII file format. This process is applicable for your state if the State Business Rule EOD_BANKINGPAIDFILEIMPORT = 'Y'.

Process Banking Paid File

If EOD_BANKINGPAIDFILEIMPORT = 'Y' and a Banking Paid file is located in the \\<STATECODE>EOD\BANKING\ directory, the End of Day Process will Add/Update Food Instrument Paid/Rejected data in the associated Food Instrument tables. Refer to Chapter 05 – Banking Files (ASCII) (EOD).doc for specifics on the ASCII file layout. If an import file is found then it will be processed, if not the process is bypassed. If multiple import files are found for a process then the import files will be processed in order from oldest to newest based on import file date and time stamp. Import files are renamed after processing so they will not be processed more than once.

Import Food Instrument File

SOAP/XML import for the Food Instrument file is no longer applicable.

Export Files

The files created by the COVANSYS system are placed in specific directories for the user to locate. Some files are generated for the sole purpose of exchanging data with systems that do not have the COVANSYS front-end applications. The function of moving, copying, backing up and archiving all export files is a manual function performed by the user. The registry key for the export file directory is HKEY_LOCAL_MACHINE\SOFTWARE\PDA<STATE>VENDOR\VendorEOD\SendToDirectory.

Export Banking Price File

The End of Day process will export Peer Group Pricing data to an ASCII file format. This process is applicable for your state if the State Business Rule EOD_BANKINGPRICEFILEEXPORT = 'Y'.

Create Banking Price File

If EOD_BANKINGPRICEFILEEXPORT = 'Y', the End of Day Process will export the Peer Group Food Instrument Type Price data to an ASCII flat file. The file naming

convention is <STATECODE>BP#####.TXT and is stored in the \\<STATECODE>EOD\BANKING directory. Refer to Chapter 05 - Banking Files (ASCII) (EOD).doc for specifics on the ASCII file layout.

Export Banking Stamp File

The End of Day process will export Vendor Stamp data to an ASCII file format. This process is applicable for your state if the State Business Rule EOD_BANKINGSTAMPFILEEXPORT = 'Y'.

Create Banking Stamp File

If EOD_BANKINGSTAMPFILEEXPORT = 'Y', the End of Day Process will export the Vendor Stamp data to an ASCII flat file. The file naming convention is <STATECODE>BS#####.TXT and is stored in the \\<STATECODE>EOD\BANKING directory. Refer to Chapter 05 - Banking Files (ASCII) (EOD).doc for specifics on the ASCII file layout.

Export Banking Vendor File

The End of Day process will export Vendor demographics data to an ASCII file format. This process is applicable for your state if the State Business Rule EOD_BANKINGVENDORFILEEXPORT = 'Y'.

Create Banking Vendor File

If EOD_BANKINGVENDORFILEEXPORT = 'Y', the End of Day Process will export the Vendor demographics data to an ASCII flat file. The file naming convention is <STATECODE>BV#####.TXT and is stored in the \\<STATECODE>EOD\BANKING directory. Refer to Chapter 05 - Banking Files (ASCII) (EOD).doc for specifics on the ASCII file layout.

Export Banking New FI Issuance File

The End of Day process will export New FI Issuance data to an ASCII file format. This process is applicable for your state if the State Business Rule EOD_BANKINGISSUANCEFILEEXPORT = 'Y'.

Create Banking New FI Issuance File

If EOD_BANKINGISSUANCEFILEEXPORT = 'Y', the End of Day Process will export the New Food Instrument Issuance Bank data to an ASCII flat file. The file naming convention is <STATECODE>BI#####.TXT and is stored in the \\<STATECODE>EOD\BANKING. Refer to Chapter 05 - Banking Files (ASCII) (EOD).doc for specifics on the ASCII file layout.

Export Banking FI Stop Payment File

The End of Day process will export the FI Stop Payment data to an ASCII file format. This process is applicable for your state if the State Business Rule EOD_BANKINGSTOPPAYFILEEXPORT = 'Y'.

Create Banking FI Stop Payment File

If EOD_BANKINGSTOPPAYMENTFILEEXPORT = 'Y', the End of Day Process will export the Food Instrument Stop Payment Bank data to an ASCII flat file. The file

naming convention is <STATECODE>BY#####.TXT and is stored in the \\<STATECODE>EOD\BANKING directory. Refer to Chapter 05 - Banking Files (ASCII) (EOD).doc for specifics on the ASCII file layout.

Export Vendor File

The End of Day process will export the Vendor demographics data to an XML file format using SOAP methods. This process is applicable for your state if the State Business Rule EOD_VENDORFILEEXPORT = 'Y'.

Create Vendor File

If EOD_VENDORFILEEXPORT = 'Y', the End of Day Process will export the Vendor Demographics data to an XML file. The file is stored in the \\<STATECODE>EOD\VENDORREQUEST directory. Refer to Chapter 06 - SOAP_XML Files (EOD).doc for specifics on the XML file layout.

Process CDC File

If a CDC file exists in the C:\WICCCDCFiles\ Subfolders: Pediatric or Pregnancy, the End of Day process will submit the files as defined by the information listed in the COMMREQUEST table. If the SENDEMAIL value is 'Y' in the COMMREQUEST table then E-Mail will be sent along with the files to notify the CDC that the files were sent. If the SENDEMAIL value is "N" then the files are sent but no E-Mail notification is sent.

Export Dual Participation File

This process is applicable for your state if the State Business Rule EOD_EXTERNALDUALPARTICIPATION = 'Y'.

If an External Dual Participation file exists in the \\<STATECODE>EOD ExtDualPart\ directory, the End of Day process will submit the files as defined by the information listed in the COMMREQUEST table. If the SENDEMAIL value is 'Y' in the COMMREQUEST table then E-Mail will be sent along with the files to notify the State Of Oklahoma that the files were sent. If the SENDEMAIL value is "N" then the files are sent but no E-Mail notification is sent. Once the files are sent they are placed in the C:\<STATECODE>EOD ExtDualPart\Sent\ directory.

The External Dual Participation file is generated quarterly during the End of Month processing and placed in the ExtDualPart directory. The End of Day processing will detect when the new file is found and the flat file will be exported from the ITO Agency to the State of Oklahoma. The file naming convention is **DUALMMYY.DAT**.

Dual Participation File Layout

Field	Length	Type
LastName	15	Char
FirstName	13	Char
MiddleInitial	1	Char
DateOfBirth	8	Date
Address	30	Char
City	20	Char
CertStartDate	8	Date
WICStatus	1	Char
IssueDate	8	Date
State	2	Char
CertEndDate	8	Date
NextPUDueDate	8	Date
Redeemed1Date	8	Date
Redeemed2Date	8	Date
Redeemed3Date	8	Date
Redeemed4Date	8	Date
Redeemed5Date	8	Date
Redeemed6Date	8	Date
Redeemed7Date	8	Date
Redeemed8Date	8	Date
Redeemed9Date	8	Date
Redeemed10Date	8	Date
Redeemed11Date	8	Date
Redeemed12Date	8	Date
Redeemed2Date	8	Date
RedeemedEnd1Date	8	Date
RedeemedEnd2Date	8	Date
RedeemedEnd3Date	8	Date
RedeemedEnd4Date	8	Date
RedeemedEnd5Date	8	Date
RedeemedEnd6Date	8	Date
RedeemedEnd7Date	8	Date
RedeemedEnd8Date	8	Date
RedeemedEnd9Date	8	Date
RedeemedEnd10Date	8	Date
RedeemedEnd11Date	8	Date
RedeemedEnd12Date	8	Date
ITO-OR-STATE	4	Char

Calculations for computing 3 Month Rolling Average

Paper FIs Food Instrument Type Average and Maximum Price

Sum the paid amounts from FIs redeemed over the last twelve weeks (today minus twelve weeks).

Caveats: The goal is to cover all WIC approved food benefits issued on the FI. The clients are instructed to select least expensive items and the vendors are trained

accordingly. At one standard deviation, the paper FI Type food items really need to be grouped on a single FI in a manner such that the items are habitually redeemed in full more often than not. At one standard deviation, if the 50% clients are consistently not redeeming the tuna at all and only part of the carrots and beans then it is possible that the maximum price could fall short for the client who redeems the full set of full food benefits on the FI. This grouping of food benefits on a single FI to support the max price at the bank will be covered in training.

We may need to provide a variable allowing the user to choose a 1, 2, or 3 standard deviations to apply. By mathematical convention, applying one standard deviation of its average, 68.3% of your dataset is generally included. At two standard deviations, 95.4% within plus/minus these two standard deviations of your average is generally included. At three standard deviations, 99.7% of your price data is generally included.

EBT Food Item Type Average and Maximum Price

Sum the paid amounts from EBTs (FICs) redeemed over the last twelve weeks (today minus twelve weeks).

Caveats: The goal is to cover all WIC approved food benefits. The clients are instructed to select least expensive items and the vendors are trained accordingly. One standard deviation may well cover the prices at the food item level. It depends upon how disparate the price variance is in the WIC approved manufacturers products, the generic milk and juice compared to the WIC approved name brands.

We may need to provide a variable allowing the user to choose a 1, 2, or 3 standard deviations to apply. By mathematical convention, applying one standard deviation of its average, 68.3% of your dataset is generally included. At two standard deviations, 95.4% within plus/minus these two standard deviations of your average is generally included. At three standard deviations, 99.7% of your price data is generally included.

Calculation

Calculate Pricing:

Average Price = Mean Redemption Amount over twelve weeks

Maximum Price = Redemption Amount over twelve weeks plus one standard deviation

Normal Distribution of Data:

A normal distribution of data means that most of the examples in a set of data are close to the "average," while relatively few examples tend to one extreme or the other.

Standard Deviation: A measure describing how close members of a data set are in relation to each other. The standard deviation is kind of the "mean of the mean" (average variance of an average), and often can help you find a pattern in the data. The standard deviation can be found by taking the square root of the variance. If the variance is 25, the standard deviation is 5.

Square Root: One of two equal factors of a given number. For example, 5 is a square root of 25 because $5*5 = 25$. Another square root of 25 is -5 because $(-5)*(-5) = 25$. The +5 is called the principle square root of 25.

Two Variance Methods:

- biased variance and standard deviation
- unbiased variance and standard deviation

Biased or Unbiased Variance Method:

For the Unbiased Method = Divide the result by the count of items in the set of data minus 1 item (standard variance value)

For the Biased Method = Divide the result by the count of items in the set of data (forcing a result of a lower variance value or a deviated variance)

The Unbiased Variance method provides a common deviation value. You should use the Unbiased Method, because it is the standard default method, unless there is a business reason to understand and use a deviated variance

In both variance method examples in the document, you begin with all three items in the data set count to produce the mean or average value.

To determine the Biased variance value, use the full count of the items in the dataset that were used to calculate the mean (average). Because the Biased Variance Method results in a lower variance value (a deviated rate below the standard variance), you do not reduce the dataset count by one.

Terms Used:

x = one value in the set of data
(the redeemed amount)

avg(x) = the average of all the values x in your set of data, the mean

- Paper FIs: (the sum of the redeemed amounts for the last twelve weeks by peer group and food instrument type)
- EBT: (the sum of the redeemed amounts for the last twelve weeks by peer group and food item)

n = the number of values (item count) in the set of data

Business Rules:

A State Business Rule defines the number of standard deviation to apply to the mean. If the State Business Rule EOD_3MONTH_ROLLING_AVG_NBR_STD_DEVIATIONS= '1' then one standard deviation is applied.

A State Business Rule defines the variance method use when calculating the standard deviation. If the State Business Rule EOD_3MONTH_ROLLING_AVG_VARIANCE_METHOD= 'B' then the biased variance method is applied.

Formula Used:

1. Count the number of items in the set of data for the beginning value of n.
2. Find the average value of all items in the set of data. Average Price = Mean Redemption Amount over twelve weeks
3. For each value x, subtract the overall avg (x) from each x. When result is negative it means that x is below the mean.
4. Multiply that result by itself (otherwise known as determining the square of that value). The result is positive.
5. Sum up all those positive squared values.
6. For the Biased Method = Divide that result by (n).

7. For the Unbiased Method = Divide that result by (n-1).
8. Find the square root of that last number, the variance, for the value of the standard deviation of your set of data. The standard deviation is the positive square root of the variance, the mean of the mean.
9. Maximum Price = Average Price plus one standard deviation.

For the data set example {1,2,3} there are a total of three items in the set of data, therefore the value of n begins at 3

1. n=3 for the total of three items in the set of data
2. 1+2+3 = 6 for the total of the value of all items in the set of data
6 / 3 = 2 to find the average value of the set of data
3. 1-2 = -1; 2-2 = 0; 3-2 = 1
4. -1 * -1 = 1; 0 * 0 = 0; 1 * 1 = 1
5. 1 + 0 + 1 = 2
6. Biased Method: 2 / 3 = .666666666 or .667
7. Unbiased Method: 2 / 2 = 1
8. Biased Method: the square root of .667 is .8168 rounded to 82 cents
Unbiased Method: the square root of 1 is 1
9. Biased Method: 2 + .82 = 2.82 **(results in a lower variance value)**
Unbiased Method: 2 + 1 = 3 **(results in a standard variance value)**

The **biased** variance is:

$$\frac{(1-2)^2 + (2-2)^2 + (3-2)^2}{(3)} = .666666666 \text{ or } .667$$

The standard deviation is the square root of the biased variance, which equals:

$$\sqrt{0.667} = .8168$$

The mean plus one standard deviation for the biased variance equals:

$$2 + .8168$$

The **unbiased** variance is:

$$\frac{(1-2)^2 + (2-2)^2 + (3-2)^2}{(3-1)} = 1$$

The standard deviation is the square root of the unbiased variance, which equals:

$$\sqrt{1} = 1$$

The mean plus one standard deviation for the unbiased variance equals:

$$2 + 1$$

Process 3 Month Rolling Average for Peer Group Pricing

An End of Day process will recalculate the peer group average and maximum prices every 2 weeks based upon actual redemption to obtain a 3-month (12 week) rolling average for the peer group food instrument type or food item. This process is applicable for your state if the State Business Rule EOD_3MONTHROLLINGAVG = 'Y'.

This calculation will not replace the manually calculated Average Price for each food item unless EBT is enabled. The manually calculated average price for each food item is needed for state office obligations, reporting and rebates when paper FIs are issued. It will replace the manually calculated Average and Maximum Prices for the Food Instrument Type and Peer Group.

Process 3 Month Rolling Average

For Paper Food Instruments:

The system will calculate the 3-month rolling average every 2 weeks by selecting issued food instruments that have been redeemed over the last 12 weeks. It will calculate the average redemption amount (the mean) within each food instrument type and vendor peer group combination and update the AvgPrice column in the PEERGROUPOODINSTTYPEPRICE table. For each vendor peer group and food instrument type it will determine the standard deviation value (the mean of the mean) and increase the maximum price by the value of one standard deviation. This information is stored in the Price column of the PEERGROUPOODINSTTYPEPRICE table.

For EBT:

The system will calculate the 3-month rolling average every 2 weeks by selecting redeemed EBT (electronic benefit transactions) over the last 12 weeks. It will calculate the average redemption amount (the mean) within each food item and vendor peer group combination and update the AvgPrice column in the PEERGROUPOODITEM table. For each vendor peer group and food item it will determine the standard deviation value (the mean of the mean) and increase the maximum price by the value of one standard deviation. This information is stored in the MaxPrice column of the PEERGROUPOODITEM table.

The AvgPrice and Price columns in the PEERGROUPOODINSTTYPEPRICE table will be updated by selecting FI with EBT redemption over the last 12 weeks, summing the peer group food item average price and max price for each food item and its quantity on the FI to set the FI Type average price and price.

APPENDIX F

NOTE: This information was supplied by Chickasaw Nation Information Technology

On-going Maintenance, Repair and Replacement of SPIRIT agency equipment

SPIRIT Agencies are responsible to replace consumable items supporting on-going maintenance of the SPIRIT equipment (e.g. toner, paper, check stock, batteries needed for e-signature pads and mice). Each agency will provide their own removable storage media (e.g. CD-R, CD-RW, DVD-R, or USB removable storage media) for copying Microsoft Office files.

The SPIRIT consortium has purchased a limited amount of spare equipment to be loaned to SPIRIT agencies while agency equipment is being repaired. Agencies experiencing equipment problems should contact the SPIRIT Help Desk immediately. The SPIRIT Help Desk staff will identify equipment problems and fixes, coordinate warranty repairs, and be the point of contact to arrange for loaners (spare equipment) to be shipped to agencies while repairs are performed.

The SPIRIT Help Desk will also work with agencies to procure computer equipment for agency expansion and/or cyclical replacements. After the initial roll out of SPIRIT equipment, any new equipment purchased for agency expansion or cyclical replacements will be funded by the agency and supported by the SPIRIT Help Desk. When new equipment needs arise, agencies are to contact the SPIRIT Help Desk. The SPIRIT Help Desk will provide equipment specifications, recommendations, and support to configure the new equipment for the SPIRIT application. All new equipment must comply with SPIRIT equipment specifications.

APPENDIX G

Setup Procedures for Data Sync

1) On the laptop setup a user called “spirit” in enterprise manager.

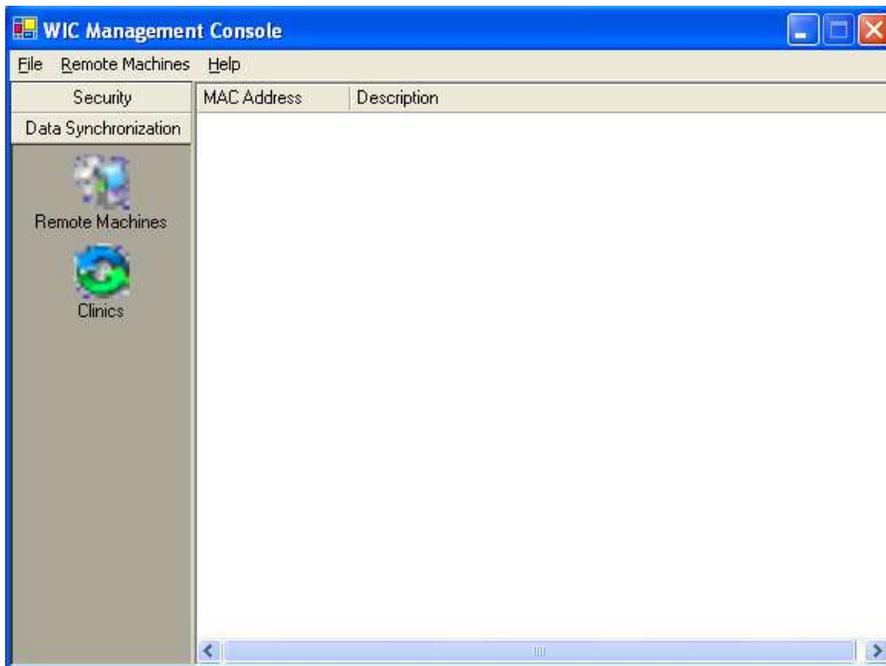


Make sure the username is set to “spirit” and the password is set to “sp1r1t76”. Also, check the System Administrators and Server Administrators boxes under the Server Roles tab.

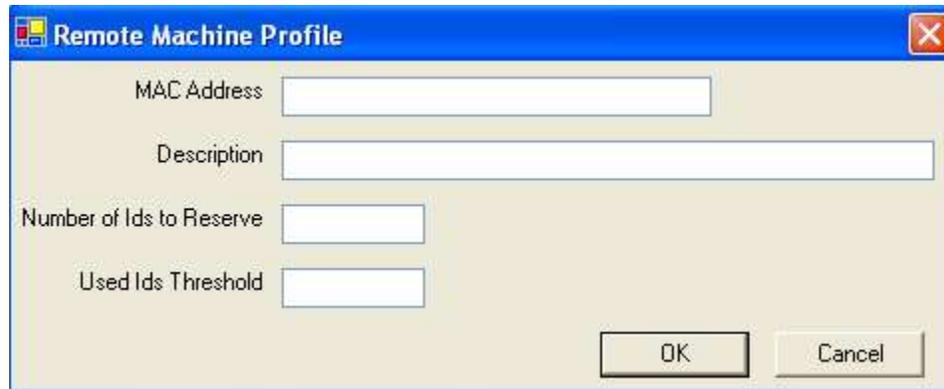
2) Make sure a current backup copy of the schema is available for the laptop to use. This backup will need to be local or on a shared network drive. Once the location of the file is determined this will need to be changed in the following file: “C:\Program Files\Covansys Inc. - BPDS\WIC\bin\DataSynchClient.exe.config”

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <appSettings>
    <add key="CheckoutCertCount" value="3" />
    <add key="CheckoutAppointmentHistory" value="3" />
    <add key="CheckoutFutureAppointments" value="4" />
    <add key="CheckoutStateWideDataCertCount" value="1" />
    <add key="DownLoadPath" value="C:\enter\your\location\here" />
  />
  </appSettings>
  ...
  ...
  ...
```

3) Open Management Console and click on the Data Synchronization.



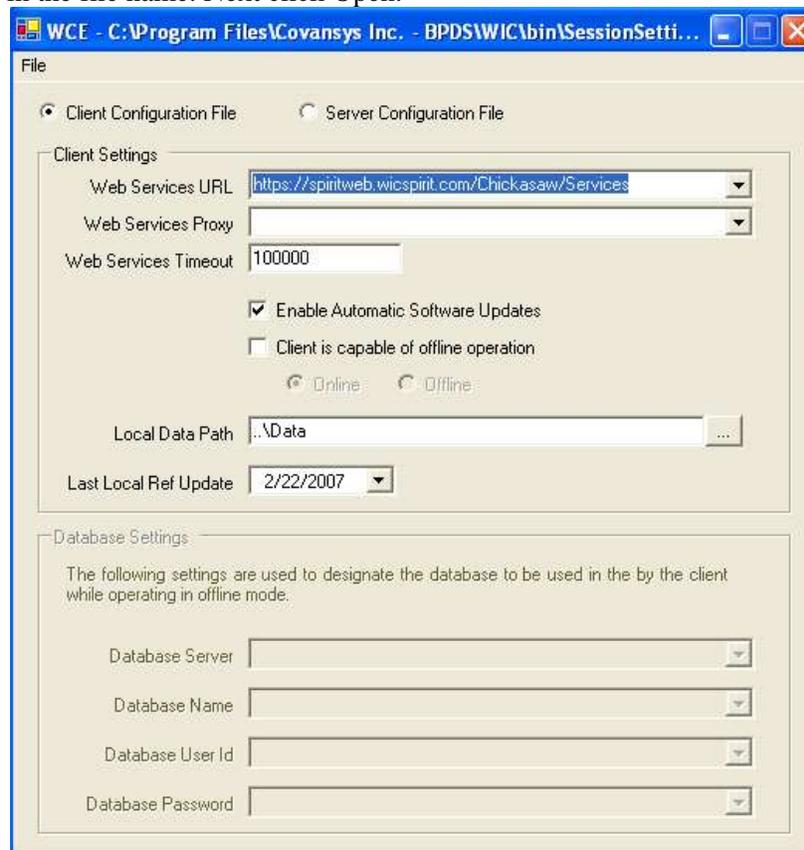
Now click on the Remote Machines button. This will change the menus. Click on the “Remote Machines” in the menu and select Add.



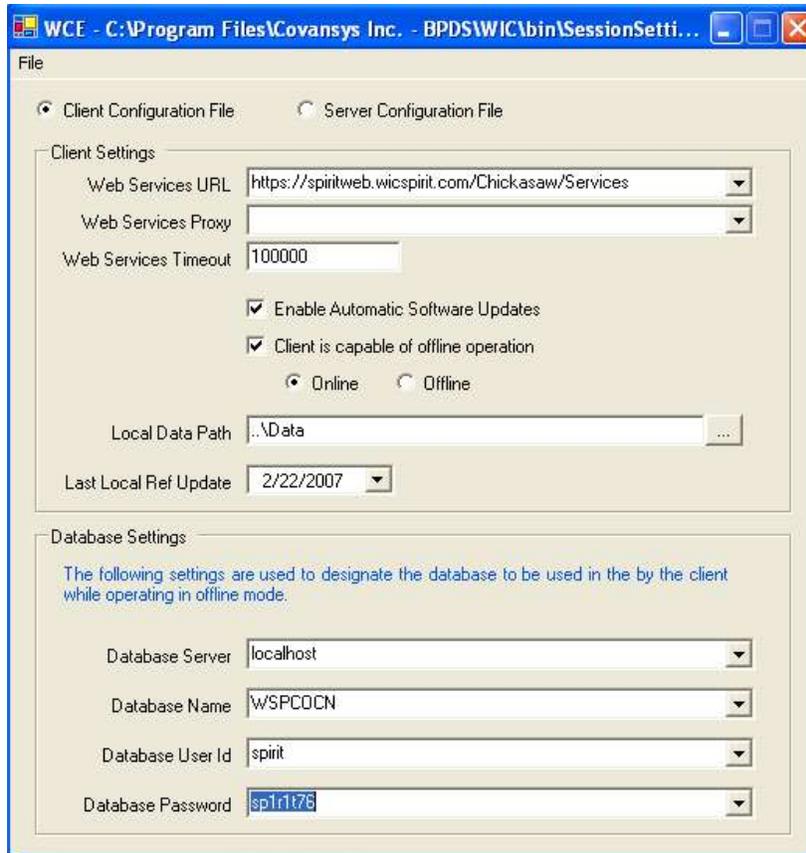
Enter the MAC address of the laptop that will perform the data sync. Note: There may be more than one MAC address. Use the appropriate address base on how the laptop is connected to the network. Next enter a Description for the laptop. Now enter the number of ID's to be reserved for off line mode and the threshold. For the average clinic 500 ID's should be reserved and 90 for the threshold

4) Setup the WIC config editor.

Click the WIC config editor icon. Once open select File and then open. The "SessionSettings.xls" should be in the file name. Next click Open.



Now check the "Client is capable of offline operation"



Next set the
 Database Server to “localhost”
 Database Name to the appropriate name

Database Name	Tribe
WSPCOAC	ACL New Mexico
WSPCOCN	Chickasaw Nation Ada, Oklahoma
WSPCOCT	Choctaw Nation Oklahoma
WSPCONP	Eight Northern Pueblos New Mexico
WSPCOSA	Five Sandoval New Mexico
WSOCOTC	Inter-Tribal Council Oklahoma
WSPCOCR	Muskogee Creek Nation Oklahoma
WSPCOOS	Osage Oklahoma
WSPCOOT	Otoe Missouriia Oklahoma
WSPCOZU	Pueblo of Zuni New Mexico
WSPCOSF	San Felipe New Mexico
WSPCOSD	Santo Domingo New Mexico
WSPCOWC	Wichita, Caddo, Delaware (WCD) Oklahoma

Database User Id to “spirit”
 Database Password to “sp1r1t76”
 Now click File-> save

- 5) Now open “Data Sync Client – Checkout” on the laptop. Select the clinic to check out and click the check out clinic button. Note the first check out will take some time. Once the check out is complete the data sync software will log the user off. The next time the user logs in they will be in the off line mode. i.e. checked out

NOTE

The LocalDB file in the C:\Program Files\Covansys Inc. - BPDS\WIC\bin directory is a backup of the sessionsettings.xml file which contains the LastDataCheckoutAt date and time.