

Prinergy 2.1

Onsite Server Integration

Document Number
72-3499B-A-PR01

4 February 2003

Creo Inc.
3700 Gilmore Way
Burnaby, BC
Canada V5G 4M1
604-451-2700

Copyright 2003 Creo Inc. All rights reserved.

Revision History

Revision	Date	Author	Comments
0.1	00-09-11	Marita Wallace	Create and format file.
0.2	00-09-26	Simon Chen	First edit and additions.
0.3	00-10-02	M. Wallace	Apply final template and copyedit draft.
0.4	00-11-21	M. Wallace	Obtain sapphire number. Attach new template. Edit and update for review.
1.0	00-11-28	S. Chen/M. Wallace	Final changes and review.
2.0	4 February 2003	Jill Thompson	Updated document for Prinergy 2.1.

CONTENTS

Revision History i

1. Introduction 1
   1.1 Related Documents 1

2. Checking Prerequisites 1

3. Preparing the Site 2

4. Unpacking the Shipment 2

5. Assembling Hardware and Connecting Devices 2
   5.1 Making Typical Prinergy SCSI Connections 3

6. Integrating Servers to the Network 3
   6.1 Changing TCP/IP Settings 3
   6.2 Editing the Hosts File 4
   6.3 Setting the Default AppleTalk Zone 4
   6.4 Setting the Adapter Network Speed and Duplex Mode 5
   6.5 Verifying Advanced Network Settings 5
   6.6 Adding Servers to a Workgroup or Domain 6
   6.7 Setting the Date and Time 7

7. Configuring Prinergy with Tertiary or File Servers 7
   7.1 Editing the SFMHosts File 8
   7.2 Adding Shared Folders in Prinergy Administrator 8

8. Configuring Remote Access 9
   8.1 Enabling the DHCP Relay Agent 10
   8.2 Granting Dial-in Permissions 10

9. Verifying pcAnywhere 11

10. Enabling Synapse InSite 3.5 to Recognize Prinergy 2.1 11

11. Reinstalling Prinergy 12

1. INTRODUCTION

This document describes the Prinergy onsite integration of a shipped, preconfigured system. A Creo service representative performs these procedures at a customer site. The Production Team will have installed Prinergy and other software as ordered on the shipped system. You can find detailed information about factory installation procedures in *Prinergy 2.1 Server Installation for Factory and Field* (72-3497B).

The *site preparation document* is usually the production order, but a presite worksheet may have additional information about the system you are installing.

This document describes one method for integrating a Prinergy system at a customer site. You may choose to install and configure each system in a slightly different sequence, depending on the environment. In some cases, changing the order may affect the success of the installation.

For more information about the recommended sequence, see the *Prinergy 2.1 Onsite Installation Checklist* (72-3498B).

1.1 Related Documents

Depending on what you need to do, check out these other Prinergy 2.1 installation procedures, available on the TechPlanet:

- *Prinergy 2.1 Server Installation for Factory and Field* (72-3497B)
- *Prinergy 2.1 Onsite Proofing Configuration* (72-3502B)
- *Prinergy 2.1 Onsite Client Installation* (72-3500B)
- *Prinergy Connect 2.x Installation Test Procedure* (72-3501A)

2. CHECKING PREREQUISITES

Ensure that the following prerequisites have been met prior to starting the system integration:

- The customer site is ready for Prinergy.
- All documents are on hand.
- The customer has completed training.
- The customer team is ready for the installation.
- Time and availability plans have been made with the customer.

See the *Prinergy 2.1 Onsite Installation Checklist* (72-3498B) for more details about each of these prerequisites.

3. PREPARING THE SITE

A number of site requirements must be met before you begin unpacking and setting up the system components. Check the *site preparation document* for specific information about the following elements:

- power requirements
- environmental factors (such as dust, static, humidity)
- space requirements

Ensure that these network conditions have been met:

- there is a dedicated direct dial phone line
- the network drop is live and going to the appropriate hub

4. UNPACKING THE SHIPMENT

1. Before unpacking the shipment, ensure that the shipping package is intact.

   CAUTION: If the package is damaged in any way, do not proceed with the installation and contact Creo or Heidelberg immediately.

2. Ensure that equipment is at room temperature before unpacking the shipment. This is especially important if the outside temperature is extremely hot or extremely cold.
3. Move the equipment to the approximate final location before unpacking. This will minimize the possibility of damaging the equipment or misplacing components.
4. Unpack the equipment, checking items against the packing slip to make sure you have received everything. If there are any missing items, make a note and contact Creo or Heidelberg immediately.

   Note: Retain all packaging materials in case anything needs to be returned.

5. Confirm that the equipment is operational by doing a simple power-on test.

   CAUTION: If the equipment appears to be damaged, contact Creo or Heidelberg immediately.

5. ASSEMBLING HARDWARE AND CONNECTING DEVICES

1. Assemble each server and workstation.
2. Connect each server and workstation to the network.
3. Connect peripheral devices.

Peripheral devices may include RAIDs, backup tape devices, archiving tape devices, proofing devices, and output devices. The *site preparation document* should specify what hardware and devices will be used for this system. For information about where to connect devices, see *Section 5.1, Making Typical Prinergy SCSI Connections*.

4. Power on the system.

5.1 Making Typical Prinergy SCSI Connections

Prinergy hardware may have multiple SCSI connections. The Production Team has labeled these connections on primary and secondary servers during the factory installation of Prinergy.

For information about how to connect Dell servers, see *Dell Server Hardware Setup For Prinergy 2.x* (72-3572A).

6. INTEGRATING SERVERS TO THE NETWORK

This section describes how to verify configurations and integrate servers (including render stations) on the customer's network. Perform this procedure on the primary server and each secondary server in the Prinergy system.

6.1 Changing TCP/IP Settings

The system was set up with a default address; you must change this address to integrate the system on the network. It is recommended that you use static addresses. If you use DHCP, there could be problems if the server's IP address changes; you must remember to edit the **hosts** file to reflect any IP address changes.

To change the TCP/IP settings:

1. Log in as an Administrator.
2. On the desktop, right click **My Network Places** and select **Properties.** The Network and Dialup Connections dialog box appears.
3. Right click **Local Area Connection** and select **Properties**. The Local Area Connection Properties dialog box appears.
4. In the **Components checked are used by this connection** box, select **Internet Protocol** and click **Properties**. The Internet Protocol (TCP/IP) Properties dialog box appears.
5. Verify that the following match the settings specified in the site preparation document or contact the network administrator:
   - **IP Address**
   - **Subnet Mask**
   - **Default Gateway** (not necessary)
   - **Preferred DNS** (not necessary)

- **Alternate DNS** (not necessary)

6. If necessary, make the appropriate changes.
7. Click **Advanced**. The Advanced TCP/IP Settings dialog box appears.
8. On the **WINS** tab, ensure that **Enable NetBIOS over TCP/IP** is checked.
9. Click **OK** twice.

6.2 Editing the Hosts File

The **hosts** file is used to translate computer host names to TCP/IP addresses. On each server, check that the **hosts** file does not contain "stale" or conflicting entries. Stale entries are entries that have not been updated to reflect IP address changes. Conflicting entries are duplicate host names mapped to different IP addresses. If an IP address has changed, whether from a DHCP server or changed manually, there may be conflicting entries.

Note: Any entries that have the comment Added by Araxi, do not delete can be safely deleted or just commented out, despite what the comment says. This is just meant to ward off people who don't know what they're doing from editing the file. The entries will get regenerated over time.

To edit the hosts file (usually not required):

1. Open the **D:\WINNT\SYSTEM32\DRIVERS\ETC\Hosts** file in Notepad.
2. Enter the Host name and IP address of all the participating servers that will be working with Prinergy.
3. Remove any entries that conflict with the current IP address of the servers. Make sure you do NOT remove the **'127.0.0.1 localhost'** entry. If it is missing, add it back in.

CAUTION: When saving the file, do not use the .txt extension.

No reboot is necessary for these changes to take effect.

6.3 Setting the Default AppleTalk Zone

A zone is a logical grouping of resources, such as servers and printers. Multiple zones are not necessary but make it easier to find devices from the chooser. All Prinergy servers including tertiary and file servers should be in the same zone if possible.

Note: Do not exceed 253 AppleTalk nodes on one network. If this number is exceeded, you may not see the server from the chooser.

To set the AppleTalk zone:

1. Log in as an Administrator.
2. On the desktop, right-click **My Network Places** and select **Properties.** The Network and Dialup Connections dialog box appears.
3. Right-click **Local Area Connection** and select **Properties**. The Local Area Connection Properties dialog box appears.
4. In **Local Area Connection Properties**, select **AppleTalk Protocol** and click **Properties**. The AppleTalk Protocol Properties dialog box appears.
5. In the **This system will appear in zone** box, select the desired zone. If there are no zones listed, this just means that the site has one zone.
6. Click **OK**.

6.4 Setting the Adapter Network Speed and Duplex Mode

By default, the network adapter is set to **Auto-Detect** the link speed and duplex mode. Incorrectly set network cards may result in slow network performance. There is no one correct setting; it depends on how the switch is configured onsite. Some switches actually give better performance in auto-detect mode, but it may be safer to explicitly select a setting. Some switches reset to factory defaults if there is a power failure.

In most cases, setting to **Auto-Detect** should give acceptable results, but you should confirm transfer rates using the Netperf utility. For information about Netperf, see *Using the NetPerf Utility* (72-3661A). Change the setting as necessary to get good transfer rates.

To configure the network card adapter:

1. In the Local Area Connection Properties dialog box, click **Configure**. The Adapters Properties dialog box appears.
2. On the **Advanced** tab, under **Property**, select **Link Speed and Duplex**.
3. In the **Value** box, select the setting best suited for the network.
4. Click **OK**.

6.5 Verifying Advanced Network Settings

Adapter order, protocol binding order, and provider order should have been set correctly in Production, but you can double-check the settings now. If these setting are incorrect, it will affect network performance.

1. On the desktop, right-click **My Network Places** and select **Properties**. The Network and Dialup Connections dialog box appears.
2. From the **Advanced** menu, select **Advanced Settings**. The Advanced Settings dialog box appears.

3. On the **Adapters and Bindings** tab, in the **Connections** section, ensure that the **Local Area Connection** is listed above **[Remote Access connections]**. If it is not, use the up and down arrow keys to change the order.

4. In the **Bindings for Local Area Connection** section, ensure **Internet Protocol (TCP/IP)** is listed above **NetBEUI Protocol** for both **File and Printer Sharing** and **Client for Microsoft Networks**. If it is not, use the up and down arrow keys to change the order.

   Note: If Hummingbird is installed, the provider order must be changed. See *Unix Connectivity to Prinergy 2.0* (72-3529A).

6.6 Adding Servers to a Workgroup or Domain

During factory installation, servers are set up in a default workgroup. Onsite, the servers must be added to the customer's workgroup or domain. All servers should be in the same workgroup or domain.

Prinergy has been tested to work with Active Directory Domains. If you are adding the server to a domain, you may need the network administrator's assistance for access to the Domain Controller.

To change the workgroup or domain:

1. Log on as an administrator.

2. On the desktop, right-click **My Computer** and select **Properties**. The **System Properties** dialog box appears.

3. On the **Network Identification** tab, click **Properties**. The Identification Change dialog box appears.

   Note: Do not change the computer name, as there are many references to the server name. It is possible to change the server name, but it is not within the scope of this document.

4. In the **Member of** section, select one of the following:

   a. If you are in a workgroup environment, select **Workgroup**.

   b. If you are in a domain environment, select **Domain**.

5. Type the domain or workgroup **name** in the appropriate box.

6. Click **OK**.

   a. If you have added the server to a workgroup, you will be greeted with a Network Identification dialog box welcoming you to the workgroup. Click **OK**. A Network Identification dialog box appears.

   b. If you are adding the server to a domain, the Domain Username and Password dialog box appears. Enter the **name and password** of an account with permission to join the domain. You may need to contact the Network administrator. Click **OK**. You will be greeted with a Network Identification dialog box welcoming you to the domain.

7. Reboot the server.

6.7 Setting the Date and Time

Ensure the time, date, and time zone are correct for each server. Scheduled backups depend on these settings.

1. From the **Start** menu, select **Settings > Control Panel > Date/Time**. The Date/Time Properties dialog box appears.
2. On the **Date & Time** tab, set the appropriate date and time.
3. On the **Time Zone** tab, select the current time zone, and then click **OK**.

7. CONFIGURING PRINERGY WITH TERTIARY OR FILE SERVERS

Once you have integrated the primary and secondary servers on the network, you are ready to configure tertiary servers and file servers.

A **tertiary server** is a Windows or Unix server that is connected to the Prinergy system, but is not running any Prinergy software components. It is used to store job folders and/or input files for Prinergy jobs and can be configured with Prinergy Administrator.

A **file server** is a Windows or Unix server that is connected to the Prinergy system, but is not running any Prinergy software components. It is used to store input files for Prinergy jobs, but does not store job folders.

Note: It is the customer's responsibility to manage tertiary and file servers. They are not covered under the Creo service contract. You should NOT install any service packs or administer their systems.

The customer should ensure that the following tasks are completed:

- Create the Araxi Service login account and add it to the local administrator group.
- Ensure TCP/IP is configured properly.
- Create folders and shares used for file input or job storage.

Detailed information about managing tertiary and file servers is available in the *Prinergy 2.1 System Administration Guide* (03-4116F) – *Chapter Three, Configuring and Managing Prinergy*.

7.1 Editing the SFMHosts File

The **SFMhosts** file is conceptually similar to the TCP/IP hosts file used for translating from host name to IP address. The SFMhosts file maps Services For Macintosh (SFM) server names to Windows server names. By default, SFM server name and window name are the same.

Why do we need this translation? Since Prinergy is a client-server system, the Macintosh client and the server have to be able to reference the same file. The Macintosh client accesses files through AppleTalk and the server must translate the reference to a UNC path so that it can access the same file.

You must add an entry to the SFMhosts file if:

- The SFM server name does not match the Windows server name.
- The tertiary or file server is not in the same zone as the Prinergy server.

To modify the SFMhosts file:

1. Open the **%AraxiHome%\etc\SFMHosts** file in Notepad.
2. Add an entry to the **[/etc/sfmhosts]** section with the following format:

   "zone:sfmservername"="ntservername"

   If there are no zones, enter **"*"** for the zone.

   CAUTION: When saving the file, ensure that you do not use the .txt extension.
3. Restart Prinergy for the changes to take effect.

7.2 Adding Shared Folders in Prinergy Administrator

In order for Prinergy to use the tertiary or file server shares, you must add the shares in Prinergy Administrator. The tertiary server must also be added to the server list.

To add a tertiary server:

1. Launch Prinergy Administrator.
2. From the **Tools** menu, select **Configure System**. The Configuration Options dialog box appears.
3. On the **Servers** tab, next to the **Tertiary Servers** box, click **Add Server**.
4. Using the UNC path, type the name of the tertiary server you want to add.
5. Click **OK**.

To add a shared folder:

1. In Prinergy Administrator, from the **Tools** menu, select **Configure System**. The Configuration Options dialog box appears.
2. On the **Shared Folder** tab, in the **Network** box, browse to the shared folder.
3. Click **Add Folder**.

8. CONFIGURING REMOTE ACCESS

The ability to dial in and remotely manage servers is a key part of servicing the Prinergy system. It is important to ensure that Remote Access Server (RAS) is properly configured and tested.

RAS should accept both NetBEUI and TCP/IP protocols. TCP/IP is our primary protocol. It is critical that TCP/IP is configured properly because some remote tools rely on it. For TCP/IP there are two choices when configuring RAS: to use a static pool or a DHCP server. A static IP address pool is preferred because it eliminates our dependency on the DHCP server.

In the factory, RAS is configured to use a **static pool** with a temporary range of addresses. It must be changed to reflect the customer's network environment. IP addresses for the static pool must be in the same subnet as the LAN connection, that is, the connection bound to the network card. If you are using a static address pool, you will need **two consecutive IP addresses** in the same subnet as the LAN interface, available from the network administrator.

If for some reason you decide to use **DHCP**, the non-preferred method, the RAS server can lease up to **three addresses**.

To configure remote access:

1. In the **Routing and Remote Access MMC**, right-click the server name (local) and select **Properties**.
2. On the **General** tab, uncheck **Router.**
3. On the **IP** tab, check the following:
   - **Enable IP forwarding**
   - **Allow IP-based remote access and demand dial connections.**
4. If you are using DHCP, in the **IP address assignment** section, select **Dynamic Host Configuration Protocol**, and then click **OK**.
5. If you are using a static address pool:
   a. Select the address range created at the factory and click **Edit**. The Edit Address Range dialog box appears.

b. Enter the **Start and End IP address**. You will need two consecutive IP addresses and they must be in the subnet and the LAN address.

c. Click **OK** and continue to *Section 8.2, Granting Dial-in Permissions.*

8.1 Enabling the DHCP Relay Agent

The Dynamic Host Configuration Protocol (DHCP) relay agent sends DHCP messages between DHCP clients and DHCP servers on different IP networks. As a factory default, RAS is set up to use a static pool and the DHCP agent is disabled. DHCP must be enabled if you decided to use it to assign IP address to RAS clients.

To enable the DHCP relay agent:

1. In the **Routing and Remote Access MMC**, expand **IP routing**, right-click **DHCP Relay Agent**, and select **Properties.** The DHCP Relay Agent Properties dialog box appears.
2. In the **Server Address** box, type the DHCP server address and click **Add**.
3. Click **OK**.
4. In the right window, in the **Interface** column, right-click **Internal** and select **Properties**. The Internal Properties dialog box appears.
5. Check **Relay DHCP packets**.
6. Click **OK**.

8.2 Granting Dial-in Permissions

After RAS is installed and configured, you must specify from which users the remote access server can accept a connection. To simplify the configuration, we will not be using Remote Access policies or granting RAS permission to domain users. Dial-in permissions are granted to the local administrator and CreoService account at the factory. You can use the following procedure to grant dial-in permissions to other accounts.

1. On the desktop, right-click **My Computer** and select **Manage**. The Computer Management MMC dialog box appears.
2. In the console tree, expand **Local Users and Groups** and select **Users**.
3. In the right window, right-click the **Administrator account** and select **Properties**. The Administrator Properties dialog box appears.
4. On the **Dial-in** tab, in the **Remote Access Permissions** section, select **Allow access**.
5. Click **OK**.
6. Repeat steps 2 –5 for the CreoService account.
7. Repeat steps 2-5 for any additional user accounts.

9. VERIFYING PCANYWHERE

pcAnywhere (PCA) is remote control software that takes control of the remote host's desktop. It is a GUI interface that lets you control the host as if you where there. This gives Creo service the ability to monitor and diagnose problems as if we were on site.

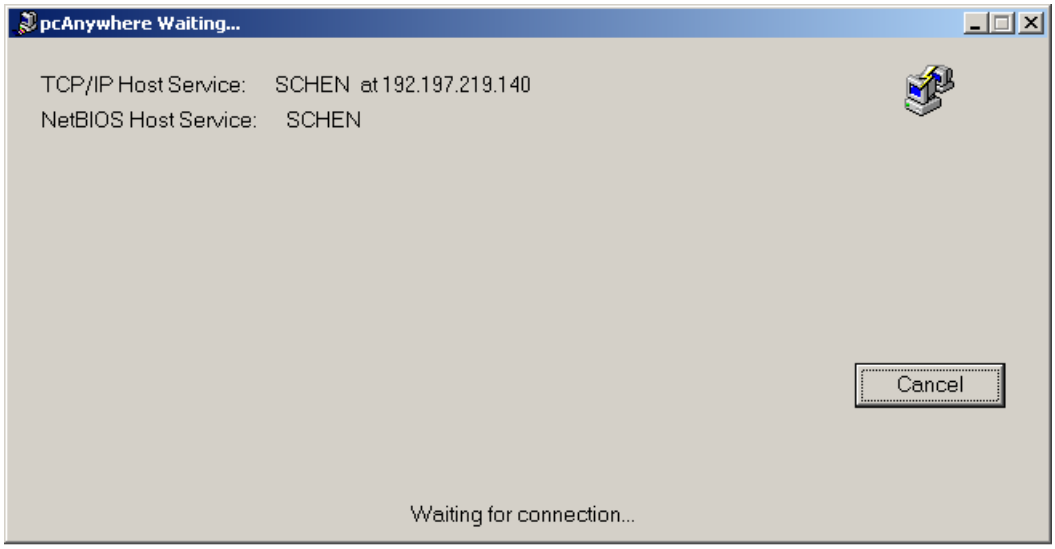
There are two versions of PCA:

- a host version running on the server to be controlled
- a client version used to control the host

PCA is installed in the Windows 2000 ghost image so it should already be part of every system. It must be reconfigured to allow full access to all callers. This should not pose a security risk because the service is set to manual. There are already several layers of security that must be passed before you can start the PCA service. You must dial in using an account that has dial-in permission, be authenticated as an administrator, and start the PCA service, before connecting with the pcAnywhere client.

To confirm the pcAnywhere configuration:

1. From the **Start** menu, select **Programs** > **Symantec pcAnywhere**. The pcAnywhere window opens.
2. In the lower frame, double-click the **Network** icon. The pcAnywhere icon should be displayed in the system tray.
3. Click the **pcAnywhere** icon. The pcAnywhere Waiting status box appears. It should indicate that both TCP/IP and NetBIOS are listening.



10. ENABLING SYNAPSE INSITE 3.5 TO RECOGNIZE PRINERGY 2.1

If Synapse InSite 3.5 is installed at the customer site prior to integrating the Prinergy 2.1 system, you must run the InSite Field Integration script to enable InSite 3.5 to recognize the Prinergy system.

1. On the server on which InSite is installed (this may be a primary, secondary, or stand-alone server), from the **Start** menu, select **Run**. The Run dialog box appears.

2. In the **Open** box, type `cmd`, and then click **OK**. A command prompt window appears.

3. At the prompt, type `net stop insite & net stop w3svc`, and then press ENTER. This stops the InSite service.

4. At the prompt, type one of the following:

   - If InSite 3.5.2 is installed (you can verify the InSite version by checking the InSite Administration home page), type
     `%CREOHOME%\support\bin\fieldintegration.cmd <username> <password> <Prinergy_primary>.`

   - If InSite 3.5.3 or later is installed, type
     `%INSITEHOME%\support\bin\fieldintegration.cmd <username> <password> <Prinergy_primary>.`

   where:

   - `<username>` is the account that InSite uses (generally `ARAXI`)

   - `<password>` is the password of the InSite account (generally `ARAXI`, case sensitive)

   - `<Prinergy_primary>` is the name of the Prinergy primary server

   For example,

   ```
   %INSITEHOME%\support\bin\fieldintegration.cmd ARAXI ARAXI YCS123-45
   ```

5. Press ENTER.

   A large amount of text may appear in the command prompt window as the script runs. This is normal.

6. When the script is finished, type `net start insite`, and then press ENTER. This restarts the InSite service.

InSite 3.5 now recognizes the Prinergy 2.1 system.

11. REINSTALLING PRINERGY

If you encounter problems while at the customer site and need to reinstall Prinergy on a primary or secondary server, refer to the instructions in *Prinergy 2.1 Server Installation for Factory and Field* (72-3497B).