

Prinergy 2.0 Installation

Onsite Server Integration

Document Number
72-3499-A-A-PR01

2000-11-28

CreoScitex
3700 Gilmore Way
Burnaby, BC
Canada V5G 4M1
(604) 451-2700

Copyright 2000 Creo Products Inc. All rights reserved.

This page intentionally left blank.

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.

This page intentionally left blank.

CreoScitex™

Prinergy 2.0 Installation
Onsite Server Integration

CONTENTS

1. Introduction 1

2. Before system integration starts 1

3. Preparing the site & unpacking the system 2
3.1 Preparing the site 2
3.2 Unpacking the shipment 2

4. Assembling hardware and connecting devices 3
4.1 Making typical Prinergy SCSI connections 3

5. Integrating servers to the network 3
5.1 Changing TCP/IP settings 3
5.2 Editing the hosts file 4
5.3 Setting the default AppleTalk zone 5
5.4 Setting the adapter network speed and duplex mode 5
5.5 Verifying advanced network settings 5
5.6 Adding servers to a workgroup or domain 6
5.7 Setting the date and time 7

6. Configuring Prinergy with tertiary or file servers. 7
6.1 Editing the SFMHost file 8
6.2 Adding shared folders in Prinergy Administrator 8

7. Configuring remote access 9
7.1 Enabling DHCP relay agent 10
7.2 Granting dial-in permissions 10

8. Verifying pcAnywhere 11

This page intentionally left blank.

1. INTRODUCTION

This chapter describes the Prinergy onsite integration of a shipped, preconfigured system. A CreoScitex 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 2.0 Factory Installation (#72-3497A)*.

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

About this procedure

This procedure describes one method for installing a Prinergy system. 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 2.0 Onsite Installation Checklist (#72-3498A)*.

Other related documents

Depending on what you need to do, check out these other Prinergy 2.0 installation procedures, available on the Technical Library:

Factory Installation (#72-3497A)

Onsite Proofing Configuration (#72-3502A)

Onsite Client Installation (#72-3500A)

Installation Test (#72-3501)

If you need to install Prinergy InSite, see *Prinergy InSite: Factory Installation (#72-3504A)*.

2. BEFORE SYSTEM INTEGRATION STARTS

Is the customer site is ready for Prinergy?

Are all documents on hand?

Has the customer completed training?

Is the customer tream ready for installation?

Have you made time and availability plans with the customer?

See the *Prinergy 2.0 Onsite Installation Checklist (#72-3498A)*. for more details about each of these prerequisite steps.

3. PREPARING THE SITE & UNPACKING THE SYSTEM

Once you've assembled the necessary documents and tools, the next steps are to prepare the site and unpack the system.

3.1 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

3.2 Unpacking the shipment

Once you have prepared the site and ensured that the network conditions have been met, unpack the system and check that all the necessary components have been included.

To unpack the shipment:

1. Before you unpack the shipment, check to make sure that the shipping package is intact.

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

4. ASSEMBLING HARDWARE AND CONNECTING DEVICES

Once you have unpacked the shipment and ensured everything is in order, you are ready to assemble the hardware and connect any peripheral devices. These include RAIDs, backup tape devices, archiving tape device, proofing devices, and output devices.

The *site preparation document* should specify what hardware and devices will be used for this system.

To assemble the hardware and connect devices:

1. Assemble each server and workstation.
2. Connect each server and workstation to the network.
3. Connect peripheral devices as specified in the site preparation document. For information about where to connect devices, see *Typical Prinergy SCSI Connections*, next.
4. Power on the system.

4.1 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 2400, 4400, and 6400 servers, see *Prinergy 2.0 Hardware and Windows 2000 Installation (#72-3476A)*.

5. INTEGRATING SERVERS TO THE NETWORK

Once you've assembled the hardware, connected peripheral devices, and powered on the system, you are ready to verify configurations and integrate each primary and secondary server (including render stations) on the customer's network.

Note: Repeat the following procedure on the primary server and each secondary server in the Prinergy system.

5.1 Changing TCP/IP settings

The system was setup with a default address and you must change it to integrate the system on the network. It's recommended that you use static addresses because Prinergy automatically updates the **hosts** file to optimize Orbix performance. If you use DHCP, there could be potential problems if the server's IP address changes. You must remember to edit the host 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 on **My Network Places** and select **Properties.** The Network and Dialup Connections window opens.

3. Right click on the **Local Area Connection** and select **Properties**. The Local Area Connection Properties dialog box opens.
4. In the **Components checked are used by this connection** box, select **Internet Protocol** and click on **Properties**. The Internet Protocol (TCP/IP) Properties dialog box opens.
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 window opens.
8. Click on the **WINS** tab. Ensure that **Enable NetBIOS over TCP/IP** is checked.
9. Click **OK** twice.

5.2 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. Prinergy automatically updates the host to optimize Orbix performance, but if the IP address has changed, whether from a DHCP server or changed manually, there may be conflicting entries.

Note: Any entries that have a comment saying, **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 and doing bad things. The entries will get regenerated over time.

To edit the hosts file:

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.

Note: No reboot is necessary for these changes to take effect.

5.3 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 server 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 on **My Network Places** and select **Properties.** The Network and Dialup Connections dialog box opens.
3. Right-click on **Local Area Connection** and select **Properties**. The Local Area Connection Properties dialog opens.
4. In **Local Area Connection Properties**, select **AppleTalk Protocol** and click on **Properties**. The AppleTalk Protocol Properties window opens.
5. In **This system will appear in zone** field, select the desired zone. If there are no zones listed., this just means that the site has one zone.
6. Click **OK**.

5.4 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 (Technical Library, Networking site, under Windows NT, Tools)*. Change the setting as necessary to get good transfer rates.

To configure the network card adapter:

1. In the **Local Area Connection Properties**, click **Configure**. The Adapters Properties window opens.
2. Click the **Advanced** tab and in the **Properties** window, select **Link Speed and Duplex**.
3. In the **Value** field, select the setting best suited for the network.
4. Click **OK**.

5.5 Verifying advanced network settings

In this step we will be checking:

- adapter order
- protocol binding order
- provider order

These setting should be correct from the factory but it doesn't hurt to double check. If these setting are incorrect, it will affect network performance.

To verify advanced network settings:

1. On the desktop, right-click on **My Network Places** and select **Properties**. The Network and Dialup Connections window opens.
2. In the **Advanced** menu, select **Advanced settings**. The Advanced Settings dialog box opens.
3. Select the **Adapters and Bindings** tab.
4. In **Connections**, ensure that the **Local Area Connection** is on top of **[Remote Access connection]**. If it is not, use the up and down arrow keys to change the order.
5. In **Bindings for Local Area Connection**, ensure **Internet Protocol (TCP/IP)** is on top of **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 will need to be changed. See Prinergy 2.0 UNIX connectivity.

5.6 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. 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 workgroups or domains:

1. Logon as an administrator.
2. On the desktop, right-click **My Computer** and select **Properties**. The **System Properties** dialog box opens.
3. Click the **Network Identification** tab and select **Properties**. The Identification Change window opens.
4. 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.
5. 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**.

6. Type the Domain or Workgroup **name** in the appropriate fields.
7. Click **OK**.
    a. If you have added the server to a Workgroup, you will be greeted with a Network Identification dialog welcoming you the workgroup. Click **OK**. A Network Identification dialog box opens.
    b. If you are adding the server to a Domain, the Domain Username and Password dialog box opens. 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 welcoming you to the domain.
8. Reboot the server.

5.7 Setting the date and time

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

To set the date and time:

1. From the Start menu, select **Settings>Control Panel**. The Control Panel window opens.
2. Double-click the **Date/Time** icon. The Date/Time Properties dialog box opens.
3. Set the appropriate date and time, in the **Time Zone** tab, select the current time zone then click **OK**.

6. CONFIGURING PRINERGY WITH TERTIARY OR FILE SERVERS.

Once you've 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's 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's connected to the Prinergy system, but is not running any Prinergy software components. It's used to store input files for Prinergy jobs, but does not store job folders.

Note: It's the customer's responsibility to manage tertiary and file Servers. They are not covered under our 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 *Chapter Three, Configuring and Managing Prinergy* in the *Prinergy 2.0 System Administration Guide (#03-4116C)*.

6.1 Editing the SFMHost file

The **SFMhosts** file is conceptually similar to the TCP/IP hosts file used for translating from host name to IP address. The SFM host 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 has to translate the reference to a UNC path so it can access the same file.

You must add an entry to the SFM host 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.

6.2 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**.
3. In the **Configuration Options** dialog box, click the **Servers** tab.
4. Next to the **Tertiary Servers** box, click **Add Server**.
5. Using the UNC path, type the name of the tertiary server you want to add.
6. Click **OK**.

To add a shared folder:

1. In Prinergy Administrator, select **Tools>Configure System**.
2. In the **Configuration Options** dialog box, click the **Shared Folder** tab.
3. In the **Network** box, browse to the shared folder.
4. Click **Add Folder**.

7. CONFIGURING REMOTE ACCESS

The ability to dial in and remotely manage servers is a key part of servicing the Prinergy system. Without this ability, we would be greatly disadvantaged. 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's 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 (2) 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 (3) addresses**.

To configure remote access:

1. In the **Routing and Remote Access MMC**, right-click on the server name (local) and select **Properties**. The Server name (local) Properties window opens.
2. In the **General** tab, uncheck **Router.**
3. In the **IP** tab, check the following:
   - Enable IP forwarding
   - Allow IP-based remote access and demand dial connections.
4. If you are using DHCP:
   a. Select Dynamic Host Configuration Protocol in the IP address assignment section.
   b. 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 window opens.

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 6.2

7.1 Enabling 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 setup 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 DHCP relay agent:

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

7.2 Granting dial-in permissions

After the remote access server 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.

To grant dial-in permission to local users:

1. On the desktop, right-click on **My Computer** and select **Manage**. The Computer Management MMC dialog box opens.
2. In the console tree, expand **Local Users and Groups** and select **Users**.
3. In the right window, right-click on the **Administrator account** and select **Properties**. The Administrator Properties window opens.
4. In the **Dial-in** tab, select **Allow access** in the **Remote Access Permissions** section.
5. Click **OK**.

6. Repeat steps 2 –5 for the CreoService account.
7. Repeat steps 2-5 for any additional user accounts.

8. VERIFYING PCANYWHERE

pcAnywhere (PCA) is remote control software that takes control of the remote host's desktop. It's a GUI interface that lets you control the host as if you where there. This gives CreoScitex 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 W2K 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 pcAnywhere client.

To confirm the pcAnywhere configuration:

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

