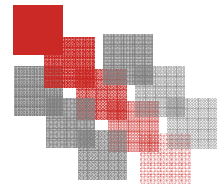


# Spherica11 PBX1 Checklist

P/N 540-351



## Spherica11 PBX1 Setup Checklist

This checklist should be used in addition to the regular Spherica11 Installation procedures and checklist. Unless otherwise noted, all items are required to make the installation PBX1 compliant.

## Servers

### 1. Ethernet NIC must support 802.1 Priority and VLAN's

- Verify that the drivers for the NIC allow you to enable layer 2 tagging.
- Enable 802.1P priority in the Ethernet driver.
- Set the VLAN ID in the Ethernet driver.

(NOTE: some installs may choose *not* to do layer 2 tagging.)

### 2. Install Spherica11

- Install Spherica11 on each server.

### 3. Commission Spherica11

- Commission Spherica11 on the Primary and all Secondary servers.
- Provide complex passwords for SPHERE-DB and SPHERE-MS accounts.
- When prompted, enter the Area Code and Main Number for your base/site.
- Select "10 digit local dialing" for the Telephony Area Template.

### 4. Enable MLPP/CallNOW

- Remove the default Outside Service address of 9 located in the Number Plan tab.
- Enable MLPP by checking the "Enable CallNOW (MLPP)" checkbox located in the CallNOW area of the General tab in System Properties.
- Assign the MLPP Domain by entering a value (up to 6 hex digits) in the MLPP Domain box located in the CallNOW area of the General tab in System Properties. Default is 0.
- Configure and enable MLPP Diversion by checking the "Set Precedence Diversion Condition" checkbox and selecting a Diversion Name/Number located in the CallNOW area of the General tab in System Properties.

### 5. Enable PBX1 Forwarding

- Enable PBX1 compliant forwarding behavior by checking the "Handset forwarded call cannot be answered by the forwarding handset" checkbox located in the Handset Forwarding Behavior area of the Call Behavior tab in System Properties.

### 6. Configure PBX1 System Settings

Add the following settings to the System Initialization Settings table located in the System initialization Settings tab in System Properties.

- G.711 CODEC Only set to true
- Jitter Buffer Size set to 1
- Sync master destination IP address set to an available multicast address
- MG Security > Access vial telnet & RDBG ... set to disabled
- MG Security > Console lock time (sec) after ... set to 60
- MG Security > Inactivity time (sec) before ... set to 60
- MG Security > Minimum lower case characters ... set to 3
- MG Security > Minimum numeric characters ... set to 1
- MG Security > Minimum password length ... set to 8
- MG Security > Minimum special characters ... set to 1
- MG Security > Minimum upper case characters ... set to 1
- Performance monitoring statistics generation ... set to disabled

### 7. Configure IP Phone Settings

Configure the following settings located on the IP Phones tab in System Properties.

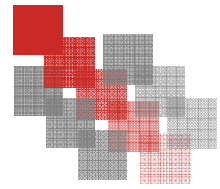
- Change the Polycom password to a complex password e.g. IpPhone1
- Check the "JITC Compliant" checkbox in the Polycom area.

### 8. Configure Spherica11 QoS

If layer 2 QoS is required for the installation then configure the following:

- Check the "Layer 2 QoS" checkbox located on the QoS tab in System Properties.
- Restart the Spherica11 Service on all servers.





## Sphere Media Gateways

### 1. CoHub MG Settings

Add the following settings to the Settings table located in the Hub tab in Hub Properties.

- MLPP Trunk Feature ... set to enabled.
- Sync master/slave for media streams ... set to master for the CoHub that will provide timing for the system.
- Sync master/slave for media streams ... set to slave for all other CoHubs.

### 2. CoHub ISDN Settings

- Verify that the ISDN Protocol is set to "National ISDN 2 wo /B channel".

### 3. Configure Layer 2 QoS

If layer 2 QoS is required for the installation then configure the following via the MG front panel switches:

- Enable support for 802.1p/q.
- Configure the VLAN ID.

## IP Phones

### 1. Polycom Phone Settings

- Configure the FTP server password to match the password entered in the server.

If layer 2 QoS is required for the installation then configure the following via the IP Phone setup menus.

- Configure the VLAN ID. Leaving it blank will disable Layer 2 QoS.

### 2. Aastra 480i Phone Settings

- Disable the Telnet Port.
- Disable the HTTP Port.

If layer 2 QoS is required for the installation then configure the following via the IP Phone setup menus.

- Enable and configure the VLAN ID.
- Enable and set the Voice Priority to 5.
- Enable and set the Control Priority to 6.

## Security

### 1. Server STIG (Security Technical Implementation Guide)

- Apply the appropriate STIG to each server i.e. Member Server or Domain Controller STIG.

### 2. Configure Local Security Policy

After applying the STIG go back and verify that the following User Rights are configured in the Local Security Policy on the Spherica11 Servers.

#### Primary Spherica11 Server

- Verify that the SPHERE-MS domain account has the local security user right **Access this computer over the network.**
  - Verify that the SPHERE-DB domain account has the local security user right **Access this computer over the network.**

#### Secondary Spherica11 Server

- Verify that the SPHERE-MS domain account has the local security user right **Access this computer over the network.**
- Verify that the SPHERE-DB domain account has the local security user right **Access this computer over the network.**
- Verify that the SPHERE-DB domain account has the local security user right **Logon as a Service.**

### 3. Configure Local Group membership

After applying the STIG go back and verify that the following domain users are members of the appropriate groups on the Spherica11 Servers.

## Spherical PBX1 Checklist

P/N 540-351



### Primary Spherical Server

- Verify that the SPHERE-MS domain account is a member of the local Administrators group.
- Verify that the SPHERESUPPORT domain account is a member of the local Administrators group.

### Secondary Spherical Server

- Verify that the SPHERE-MS domain account is a member of the local Administrators group.
- Verify that the SPHERE-MS domain account is a member of the local Administrators group.
- Verify that the SPHERESUPPORT domain account is a member of the local Administrators group.

#### 4. **Configure Security for the FTP accounts**

Configure and verify the following items on the FTP server.

- Verify that both the Sayson and PlcmSpIp FTP accounts have the local security user right **Access this computer over the network.**
- Verify that both the Sayson and PlcmSpIp FTP accounts are not members of the Guests group for the FTP server or the domain.
- Verify that both the Sayson and PlcmSpIp FTP accounts have full control of the "Program Files\Sphere\ftproot" folder on the FTP server.

#### 5. **Event Logs**

- To ensure that the Event Logs will clear and auto-archive, verify on each server that the following Registry key exists and has the correct value.

**HKLM\SYSTEM\CurrentControlSet\Services\EventLog\AutoBackupLogFiles = 1 (Dword)**

#### 6. **Disable Automatic Accounts**

- To ensure that any automatically created accounts do not get re-created verify on each server that the following Registry key exists and has the correct value.

**HKLM\SYSTEM\Software\Microsoft\Inetstp\DisableUserAccountRestore = 1 (Dword)**

#### 7. **Re-check the Server STIG**

- Use the appropriate Gold Disk to re-verify the STIG has been applied and note the exceptions created in steps 2,3,4 above.

## **Spherical Media Server**

#### 1. **Security**

If you are using Spherical Voice Mail, configure the following settings in the Media Server tab in System Properties.

- Minimum PIN Length ... set to 7
- PIN History ... set to 3
- Use Maximum Pin Age ... enabled and set to 90 days
- Use Minimum Pin Age ... enabled and set to 0 days

