

MGC WebCommander

Release Notes

Version 9.0.1



December 2007

DOC2200A

Copyright © 2007 Polycom, Inc.
All Rights Reserved

All text and figures included in this publication are the exclusive property of Polycom, Inc., and may not be copied, reproduced or used in any way without the express written permission of Polycom, Inc. Information in this document is subject to change without notice. This document also contains registered trademarks and service marks that are owned by their respective companies or organizations.

If you have any comments or suggestions regarding this document, please send them via e-mail to info@polycom.com.

Catalog No. DOC2200A
Version 9.0

Proprietary and Confidential

The information contained herein is the sole intellectual property of Polycom, Inc. No distribution, reproduction or unauthorized use of these materials is permitted without the expressed written consent of Polycom, Inc. Information contained herein is subject to change without notice and does not represent a commitment of any type on the part of Polycom, Inc. Polycom and Accord are registered trademarks of Polycom, Inc.

Notice

While reasonable effort was made to ensure that the information in this document was complete and accurate at the time of printing, Polycom, Inc., cannot assume responsibility for any errors. Changes and/or corrections to the information contained in this document may be incorporated into future issues.

Portions, aspects and/or features of this product are protected under United States Patent Law in accordance with the claims of United States Patent No: US 6,300,973; US 6,496,216; US 6,757,005; US 6,760,750; and US 7,054,620.

PATENT PENDING

Contents

Version 9.0 - New Features List.....	1
Version 9.0 Package Contents	2
MGC Web Server Requirements	2
Installing the MGC WebCommander Software Package.....	3
Backing Up the SQL/MSDE Database	3
Backing up the Access Database	5
Software Installation	5
Installation Wizard and Product Upgrade	5
Defining the MGC Web Server Security Properties	9
Selecting the User Account for Accessing the MGC Web Server	10
Starting up the Server	11
Selecting the User Account for Accessing the WAM Server	12
Starting up the WAM Server	12
Optimizing E-mail Delivery on the Server	12
Integrating Polycom PathNavigator	12
Updating the Database	12
Version 9.0 Detailed Description - MCU Redundancy and Backup	15
MCU Redundancy	15
Redundancy Guidelines	16
MCU Redundancy Configuration	17
MCU Backup	17
Defining the Backup Parameters	18
Version 9.0 Detailed Description - Secure Mode	19
Secure Mode Prerequisites	19
IIS Server - SSL/TLS Certificate Verification	20
Database Security Settings	20
Secure Mode Implementation	21
Installation Setup	21
Modifying the Security Settings in the Web Server Manager	22
Verifying the Secure Mode Settings	24
IIS Server Security Setting Verification	24
OperServ Security Settings Verification	25
DCOM Configuration	27
OperSrv Configuration for NT Authentication	27
WAM Configuration for NT Authentication	30
Allowing Connecting/Starting the Application Server (OperSrv) from Server Manager Clients	31
Manually Updating the MCU Password	33
Permissions Setting	33
Switching from Secure Mode to Non-Secure Mode	34

WebCommander Server Client Installation	35
Version 9.0 - Corrections, Limitations and Pending Issues	36
Version 9.0 Corrections	36
Corrections between Versions 8.0 and 9.0	36
Corrections between Versions 7.5 and 8.0	36
Version 9.0 System Limitations	38
Pending Issues Version 9.0	40

Version 9.0 - New Features List

The following table lists the new features in Version 9.0.

	Category	Feature Name	Description
1.	General	MCU redundancy and backup	<p>A new WebCommander Service, <i>Central Server</i> is installed as part of the WebCommander server. With this service the following functionality is added to the MGC environment:</p> <ul style="list-style-type: none">• MCU Redundancy - Automatic copying of ongoing conferences and reservations between two MCUs, so one MCU mirrors the other. When one MCU fails, it will be automatically replaced by the other MCU.• Automatic backup of MCU configuration for all MCUs defined and connected in the MCUs list of the WebCommander Server Manager. •
2.	General	Secure Mode	<p>You can configure the WebCommander application to be used in a Secure Mode using SSL/TLS.</p>

Version 9.0 Package Contents

Version 9.0 software and documentation CD includes the following items:

- MGC WebCommander software:
 - MGC Web Server
 - MGC Web Server Manager
 - WebCommander Configuration application
 - MGC Personal Scheduler Client Installation
- Documentation in PDF format:
 - MGC Web Server Manager Installation and Configuration Guide
 - MGC Web Server Manager User's Guide
 - MGC WebCommander User's Guide
 - MGC Personal Scheduler Quick Start Guide
 - Version 9.0 Release Notes

MGC Web Server Requirements

The MGC Web Server requirements are as follows:

- Pentium III, 400MHz (or higher) processor
- 256 MB RAM
- Microsoft Windows NT Server, Windows Server 2000 (Standard edition), or Windows Advanced Server 2000, Windows Server 2003 (the last three are mandatory for Japanese and Chinese language support)
- Microsoft IIS version 4.0 with Service Pack 4.0. For Japanese and Chinese language support, Microsoft IIS version 5.0 with Service Pack 1.0 is required
- Free hard disk space:
 - For MGC Web Server Manager application: 150 MB
 - For Database records: 30 MB
 - If SQL server is installed: 200 MB
- Database Software:
 - With the WebCommander and MGC Personal Scheduler it is recommended to use Microsoft SQL Server database. Microsoft Access can be used for the MGC Manager application
 - When integrating the Polycom PathNavigator database, use the Microsoft SQL Server version 7.0, SQL 2000 or SQL 2005 application. In this case, Windows NT Service Pack 4.0 or later is required
- 15" SVGA monitor, 600 x 800 pixels resolution. Recommended: 17" monitor



The MGC WebCommander client application can also be used with Vista operating system. The MGC Personal Scheduler plug-in can also be used with Microsoft IE7.

Installing the MGC WebCommander Software Package

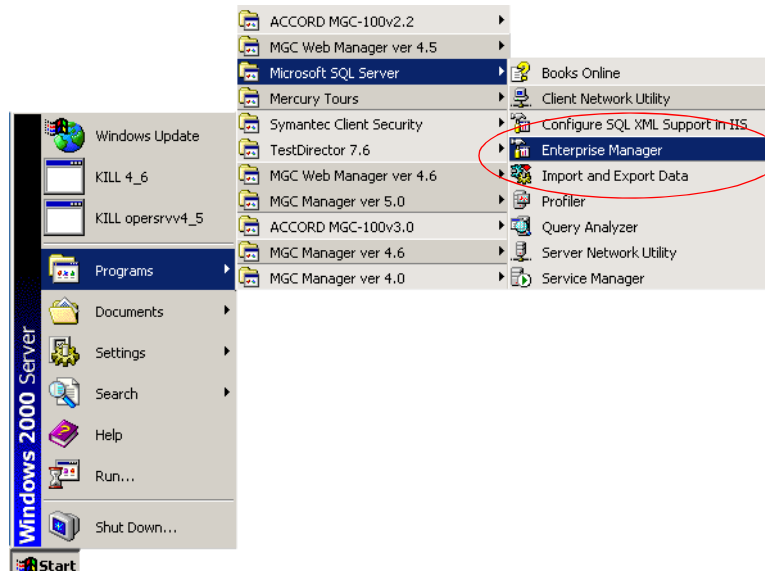
Prior to Installation and Software Upgrade

If you are upgrading from a previous version, it is recommended to backup the SQL/MSDE or Access database.

Backing Up the SQL/MSDE Database

To backup the SQL/MSDE database:

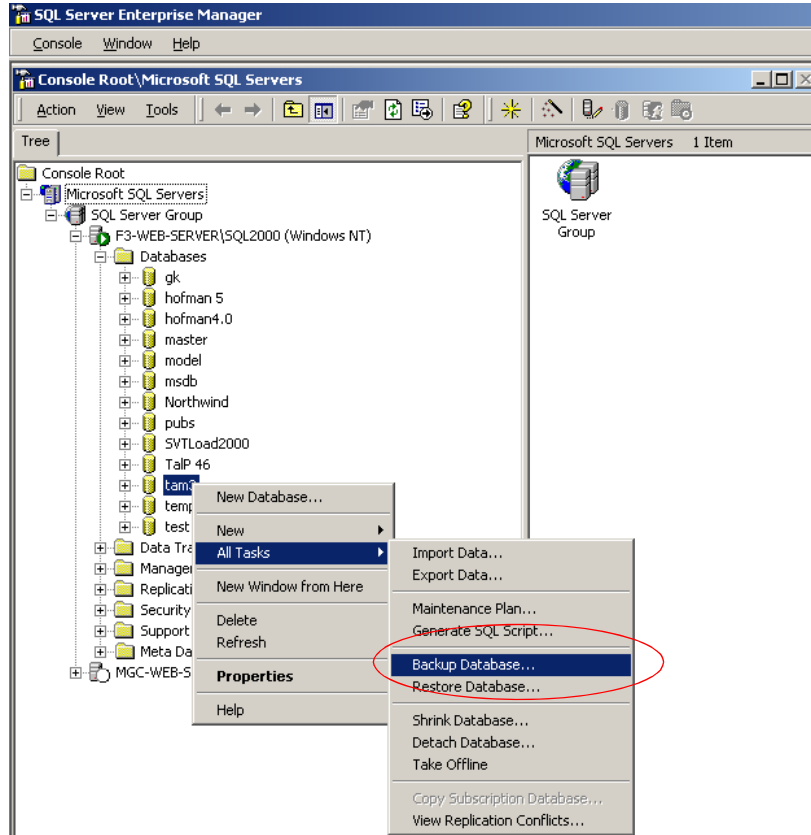
1. On the *Start-Programs* menu, click **Microsoft SQL Server** and then **Enterprise Manager**.



The *SQL Server Enterprise Manager* window opens.

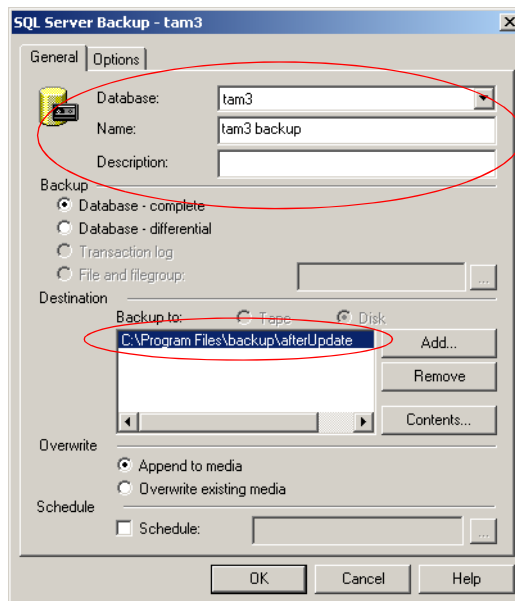
2. Expand the **Microsoft SQL Server** list.
3. Expand the **SQL Server Group** list.
4. Expand the **<PC Name>** list.

5. Right-click the *Databases* folder icon, click **All Tasks**, and then select **Backup Database**.



The *SQL Server Backup – General* dialog box opens.

6. In the *General* tab, select a database from the list, enter a name for the backup file, select a backup destination folder and click **OK**.



When the backup process is completed successful, a confirmation message is displayed, indicating the backup operation was completed successfully.

7. Click **OK**.

The new backup file is located in the destination folder selected in step 6.

Backing up the Access Database

To backup the Access database:

1. Open the folder where the database resides.
2. Select the database file by clicking it.
3. From the *Edit* menu, select **Copy**, and then select **Paste**.
4. The backup database file called *Copy of <database_name>*, appears in the same folder as the original database. This file can be moved to any folder.

Software Installation

The Installation Wizard guides you through the installation process for the MGC Web Server.

If installing from FTP:

1. Download the software from the FTP site and unzip the files.
2. Open Windows Explorer and browse to the directory that contains the MGC WebCommander diskettes.
3. Expand the **Disk 1** folder and double-click the **Setup.exe** file.

The *Installation Wizard Welcome* screen opens.

If installing from a CD:

1. Insert the CD into the CD drive.
2. From the *Start* menu, select **Run**.
3. In the Run dialog box, enter **D:Setup**, where D is the CD drive name, and then click **OK**.

The *Installation Wizard Welcome* screen opens.

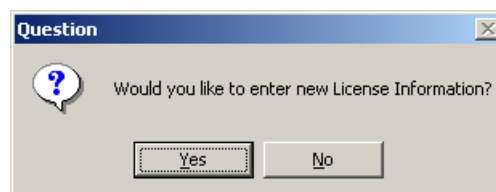
Installation Wizard and Product Upgrade



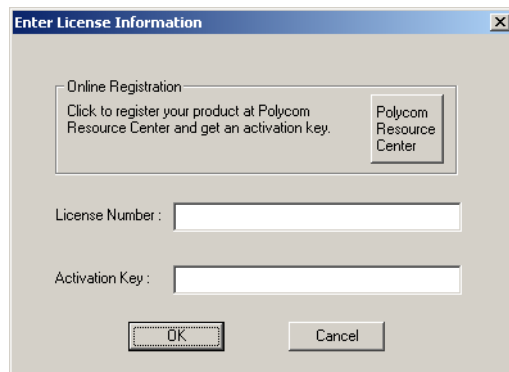
The installer must have administrator rights or domain administration rights to install software. It is also important that the password used to access the domain is permanent and does not expire after 90 days.

Follow the on-screen instructions of the installation procedure.

1. Double-click the WebCommander setup icon.
The *Question* dialog box appears, prompting you if you want to update your license information.



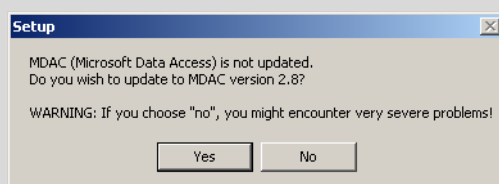
2. Click **Yes**.
The *Enter License Information* window opens.



- a. Click **Polycom Resource Center** to register your product and retrieve the software *Key Code*.
- b. In the *License* field enter the code located on the Product CD.
- c. In the *Activation Key* field enter the product code retrieved from the Polycom website.

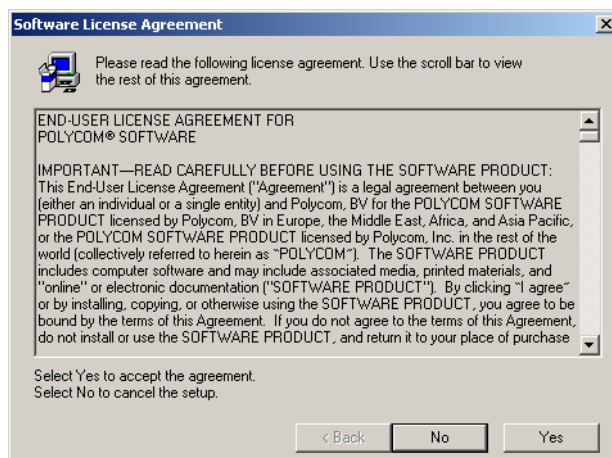


In certain instances the following dialog box appears.



Click **Yes**, to upgrade your MDAC version and continue the installation. Windows automatically reboots after the MDAC installation, and the WebCommander installation setup restarts automatically.

- d. Click **OK** and continue the installation setup.
The Software License Agreement window appears.



3. Click **Yes** to use the product and continue the installation setup.
The *Welcome* window opens.
4. Click **Next**.
The *User Information* window opens.

5. Enter the user *Name* and *Company* details and click **Next**.
The *Setup Type* window opens, listing the products according to the purchased package.
6. Select the appropriate product type as follows:



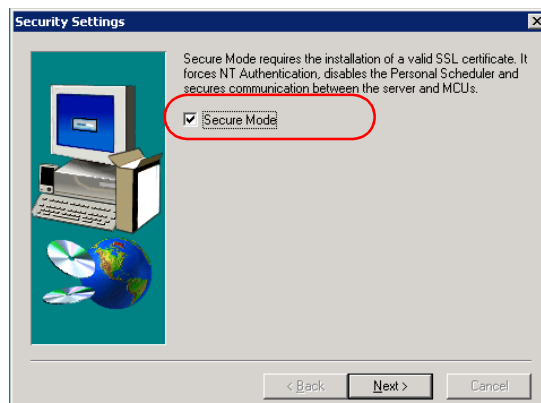
Depending on the license purchased, not all or a combination of the modules appear.

- **Client** – Installs the MGC Web Server Manager application on a computer other than the server for remote access to the MGC Web Server.
 - **Meeting Scheduler Server** – Installs the MGC Web Server and MGC Web Server Manager applications that enable users to define, modify, and start reservations via the Web or Microsoft Outlook.
 - **Meeting Director Server** - Installs the MGC Web Server and MGC Web Server Manager applications that controls and manages On Going conferences via the Web. This module enables users to monitor the ongoing conference status, and perform various operations.
 - **Professional Server** – Installs the MGC Personal Scheduler and the Meeting Director Server components to enable full functionality from the Web, and conference scheduling from Microsoft Outlook. This installation allows users to schedule and start reservations, monitor, and control On Going conferences from the Web.
7. Click **Next**.
The *Choose Destination Location* window opens.
 8. Select the target path for the installation (it is recommended to accept the suggested path and directory name) and click **Next**.
The *Select Programs Folder* window opens.
 9. Click **Next** to accept the suggested group folder and name.
The system starts downloading the software files. When the download is complete, a *Security Configuration* dialog box appears.



In Secure Mode all communications between the WebCommander components (WebCommander sites, WebCommander client, Server Manager application, OperServ, WAM and MCUs) are encrypted and authenticated.

10. In the *Security Configuration* window, select whether to implement the WebCommander's **Secure Mode** and click **Next**.





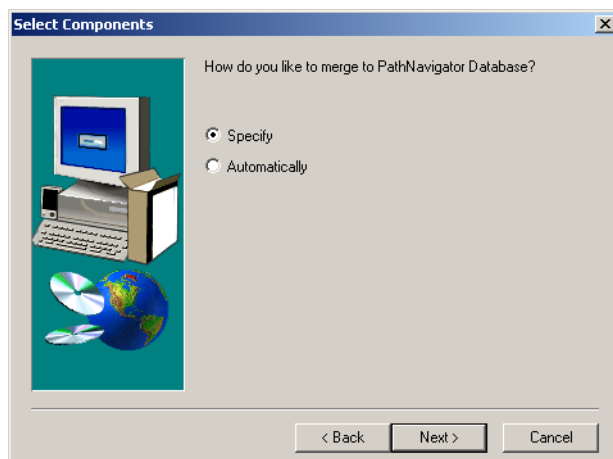
- The *Central Server Service* is disabled in Secure Mode. Leave this check box cleared if you want to use the *Central Server Service* features such as MCU redundancy, Backup and Auto Cascading.
- If you are upgrading from a non-secured installation, leave this check box cleared to install the new version in non-Secure Mode. Once the installation is complete, change the WebCommander security settings using the Server Manager application.

If you have selected the *Secure Mode* option, the *Information* dialog box opens indicating that the database must be configured to Secure Mode (if you have not done so prior to the WebCommander installation). Click Yes to continue the installation process.

- In the *Link to PathNavigator* dialog box, select whether to create a direct link to the PathNavigator gatekeeper and use its database. For more information see the *Software Installation* section in the *MGC Web Manager Installation and Configuration Guide*.

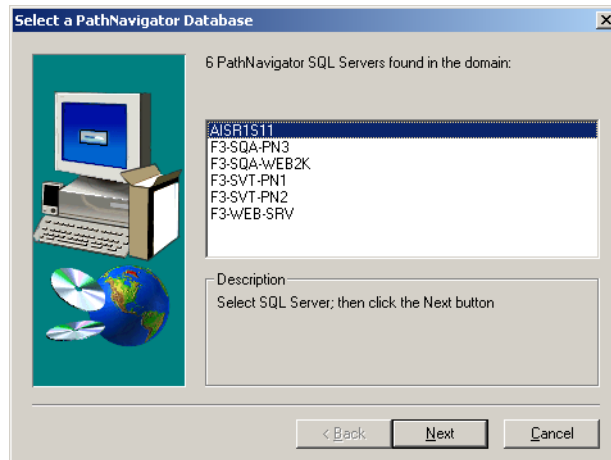
Select:

- **Yes**, to automatically configure the link to the PathNavigator gatekeeper. Proceed with step 12.
 - **No**, if no PathNavigator gatekeeper is installed in your environment, or to manually define the link to the PathNavigator. Proceed with step 14.
- If you have selected *Yes*, the *Select Components* window opens. The following options are available:

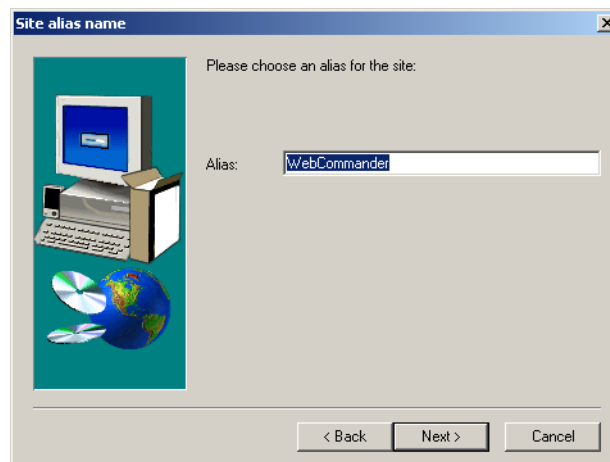


- *Specify* is the default setting. It enables you to manually define the link to the PathNavigator gatekeeper.
 - *Automatically* lets the WebCommander search for a PathNavigator database on all the SQL servers installed in the local domain and automatically create the link between them.
- Click **Next** to manually select the PathNavigator gatekeeper server. The *Enter Information* window opens.
 - Enter the name of the PathNavigator gatekeeper server, and click **Next**.
 - A confirmation dialog box (*Server found*) opens. Click **OK**.
 - Select **Automatically** to let the system to automatically detect the PathNavigator gatekeeper, and click **Next**. A confirmation dialog box opens, click **Yes**.

- c. The *Select a PathNavigator Database* dialog box appears, listing the SQL Servers found in the local domain.



13. Select the required *PathNavigator Server*, and then click **Next**.
14. The *Site alias name* window opens. Enter the site *Alias* name.



The site *Alias* name automatically redirects participants to the correct Web site in the event that the address changes (for instance, when upgrading to a higher version). For example, the alias entered to go to the Web site can be *abcABC*, where *abcABC* is the IP address of the WebCommander server.

15. Click **Next**.
The *Setup Complete* window opens.
16. Click **Finish** to complete the installation procedure and exit the Setup Wizard.



Sometimes the error message “Cannot Create Application” appears at the end of the installation. This error message may appear when there are two Web sites installed in the system. In this case, you need to manually create and configure the ConfSiteV9_0 and ConfPollerSiteV9_0 in the IIS application.

Defining the MGC Web Server Security Properties

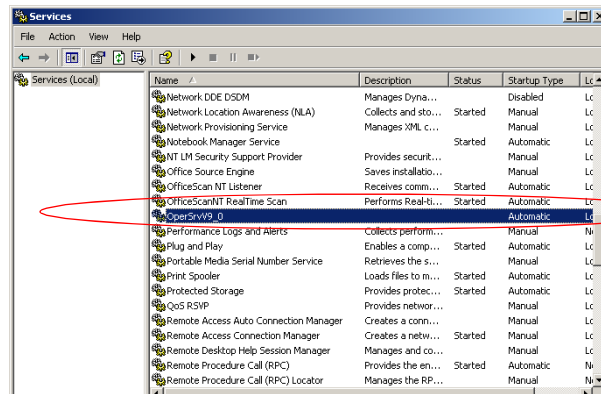
The security properties of the MGC Web Server must be defined to allow access to the Server. For more information see, *Defining the MGC Web Server Security Properties* in the *MGC Web Manager Installation and Configuration Guide, Chapter 5*.

Selecting the User Account for Accessing the MGC Web Server

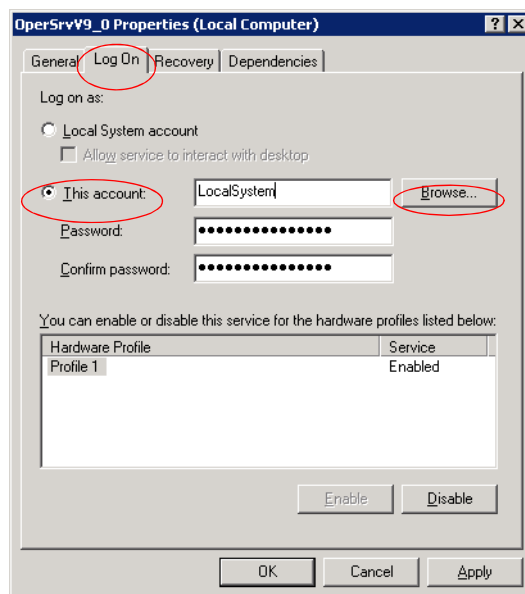
The Web Server application is installed during the WebCommander installation process. When using a local database, there is no need to define the Web Server security properties. All other database definitions require configuring the properties of the Web Server.

To select the user account in Windows NT/2000/2003 Server:

1. Click **Start > Settings > Control Panel > Administrative Tools > Services**.
The *Services* window opens.



2. Right-click **OperSrvV9_0**, and then click **Properties**.
The *OperSrvV9_0 Properties (Local Computer)* dialog box opens.
3. Click the **Log On** tab.
4. Select **This account** to select the user with access to the MGC WebCommander Server.
5. Click the **Browse** button to select the user name.



The *Select User* dialog box opens.

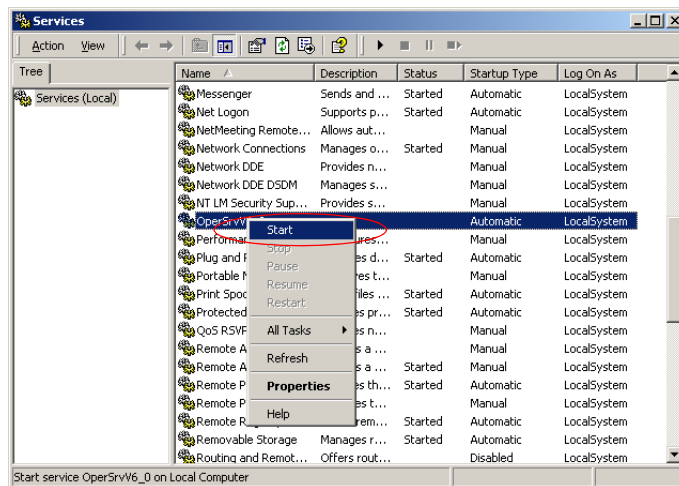
6. Select the user name from the list, and then click **OK**.
The system returns to the *OperSrvV9_0 Properties* (Local Computer) dialog box.
7. In the *Password* field, enter the user password.
8. In the *Confirm Password* field, enter the user password.
9. Click **OK**.
A confirmation box opens.
10. Click **OK** to confirm and complete this procedure.

Starting up the Server

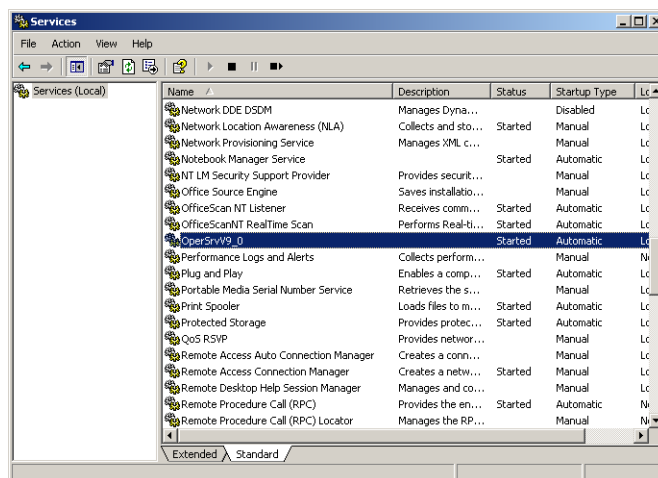
When the application is installed, the server is started automatically. A manual start of the server is only required when the password is changed or for troubleshooting.

To start up the Server in Windows NT/2000/2003 Server:

1. Click **Start > Settings > Control Panel > Administrative Tools > Services**.
The *Services* window opens.
2. Right-click **OperSrvV9_0**, and then click **Start**.



The *Service Control* box opens, indicating that Windows is attempting to start the *OperSrvV9_0* service.



In the *Services* dialog box, the status of the service changes to “Started”.

Selecting the User Account for Accessing the WAM Server

By default, the WAM Server is installed during the WebCommander installation process. When using a local database, there is no need to define the WAM Server security properties. All other database definitions require setting the properties of the WAM Server. For more information see, *Selecting the User Account for Accessing the WAM Server* in the *MGC Web Manager Installation and Configuration Guide, Chapter 5*.

Starting up the WAM Server

When the application is installed, the server is started automatically. When a PathNavigator gatekeeper is present on the network, there is no need to define the WAM Server security properties. With SQL Authentication however, configuration of the WAM server is required when no PathNavigator is present on the network. A manual start of the server is also required when the password is changed or when troubleshooting the server. For more information see, *Starting up the WAM Server* in the *MGC Web Manager Installation and Configuration Guide, Chapter 5*.

Optimizing E-mail Delivery on the Server

You can Optimize e-mail Delivery on your Server. For more information see, *Optimizing E-mail Delivery on the Server* in the *MGC Web Manager Installation and Configuration Guide, Chapter 5*.

Integrating Polycom PathNavigator

When the Polycom PathNavigator is installed in your enterprise you can access the endpoints registered with the PathNavigator via the WebCommander. For more information see, *Integrating Polycom PathNavigator* in the *MGC Web Manager Installation and Configuration Guide, Chapter 5*.

Updating the Database

When upgrading from a previous version of the MGC Web Server Manager, the old database is saved during the installation procedure.



However, it is recommended that you back-up the database before updating the database.

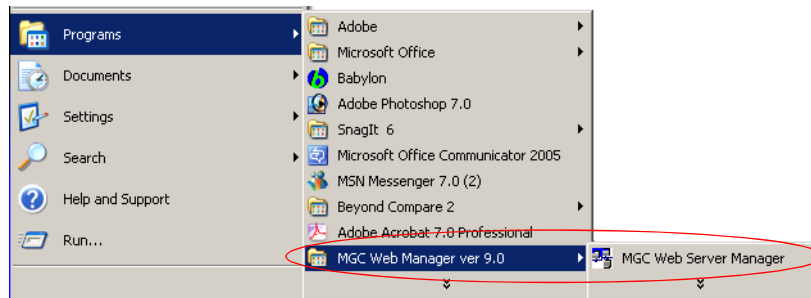
At the end of the installation procedure, you must access the MGC Web Server Manager application to automatically update the database.



The procedure for updating the database is the same for Windows 2000, Windows 2003 and Windows NT.

To update the database:

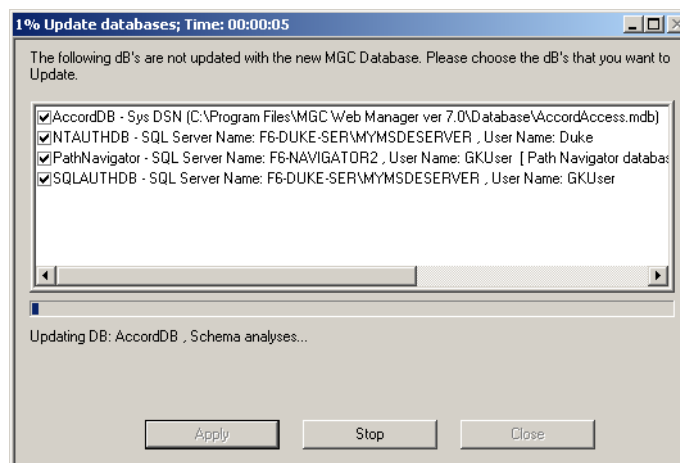
1. On the *Start – Programs* menu, click **MGC Web Manager Ver 9.0**, and then click **MGC Web Server Manager**.



The *Database Login* dialog box opens.

2. Enter your *Login Name* and *Password* as defined in the database and click **Login**. The default *Login Name* is **admin1**. The default *Password* is **123**. The system automatically starts the update process.
3. If there are discrepancies in the number of fields between the old and the new database version, the system prompts whether to update the existing database to the new format. Click **Yes** to automatically update the database (recommended), or **No** to leave the database unchanged. If you select *No*, new entries added to the database via the MGC Web Server Manager will not be saved.

If you select *Yes*, the *UpdateDB* dialog box opens, indicating which databases require updating.



4. Update all the databases you intend to use. To cancel the update of a database, clear the check mark next to the database name.
5. Click **Apply** to update the selected databases. The updating process may take time, depending on the size of the database. At the end of the process, an *Update Database Results* dialog box may open, listing the fields that were updated.



On computers that support Unicode, a dialog box does not appear.

6. Click **OK** to return to the *UpdateDB* dialog box.

7. Click **Cancel** to close the dialog box and exit the update process.



- When upgrading from a previous version which did not support Groups, the Update Database process - automatically performed by the Server Manager - creates a group for each listed user, and retains the access rights defined for a user as the access rights to that group.
- Participant templates and Conference templates are automatically assigned to the *Root* directory; therefore, only users who have access rights to the root directory (usually administrators) are able to view these conferences. The templates can be moved to the appropriate group in the Groups tree in the Database Manager segment, using Copy and Paste (drag & drop is not available).
- When you open the MGC Web Server Manager for the first time after an upgrade, and you have not yet updated the database, you can do it later using the **dB's Update** from the *Options* menu.

Version 9.0 Detailed Description - MCU Redundancy and Backup

A new WebCommander Service, *Central Server* is installed as part of the WebCommander server. With this service the following functionality is added to the MGC environment:

- MCU Redundancy - Automatic copying of ongoing conferences and reservations between two MCUs, so one MCU mirrors the other. When one MCU fails, it will be automatically replaced by the other MCU.
- Automatic backup of MCU configuration for all MCUs defined and connected in the MCUs list of the WebCommander Server Manager.

MCU Redundancy

The Central Server Service is designed to monitor the activity of assigned pairs of MCUs, so if one MCU in the pair encounters a problem that prevents it from running conferences, the other MCU will take over smoothly.

In Central Server Service environment, as described in Figure 1, MCU A and MCU B are both registered in the gatekeeper with the same prefix and they are designated as backup to each other in the WebCommander Central Server Service.

The Central Server Service monitors both MCUs. When a new on going conference is created on one MCU (for example, MCU A), the Central Server Service automatically copies this conference to the second MCU (for example, MCU B) with the prefix *bck_. In the same way, when new reservations and Meeting Rooms are created on one MCU they are automatically copied to the second MCU.

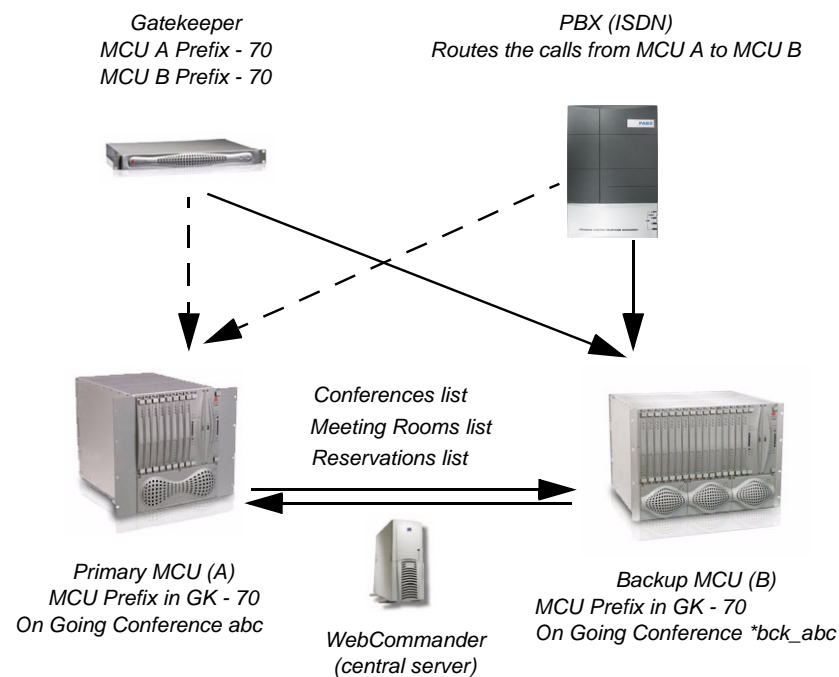


Figure 1: Central Server Service Environment

When one MCU is down (for example, power shortage), the gatekeeper will identify that one MCU (A) is unavailable and will automatically forward the calls to the second MCU (B). The participants are connected to the conference that was copied from MCU A with the same name.

When the first MCU (A) is up and running again, the gatekeeper will connect the participants to conferences running on MCU A. If a conference with the same ID is now running on both MCUs (for example, if MCU A recovered quickly, participants that connected later were connected to MCU A), the system will automatically cascade both conferences (using the Auto Cascade feature) to create one conference. This will eliminate the need to disconnect and reconnect participants to a single conference.

If the origin conference is terminated on one MCU its backup conference will be automatically terminated on the second MCU.

In the same way, if ISDN PBX is configured to route calls from one MCU to another according to MCU availability, the same behavior will occur.



The *Central Server Service* is disabled in Secure Mode.

Redundancy Guidelines

- ISDN and IP Network Services must have the same configuration (for example, MCU Prefix in gatekeeper, dial-in numbers range, etc.) on both MCUs.
- Conference Profiles, Entry Queue and IVR Services must be identical on both MCUs.
- Entry Queues must be identical on both MCUs.
- The following conference parameters are copied from the source MCU to the target MCU (backup):
 - Conference duration
 - Passwords (chairperson and conference entry)
 - User Defined fields
 - Billing Code
 - Lecture Mode parameters
 - Layout and Auto Layout
- The following conference parameters are NOT copied:
 - Remarks and Remarks History
 - Lecturer Name (as the backup conference does not include participants)
 - Video Forcing (as the backup conference does not include participants)
- If a new conference is started or scheduled on one MCU, and the MCU failed before the conference was backed up on the second MCU, this conference will not be backed up.
- Defined participants are not copied between MCUs and they must be added manually to the backup conferences.
- If the conference is cascaded, it cannot be monitored as one conference.
- If the parameters of one conference are updated, they will be automatically updated also in the backup conference.

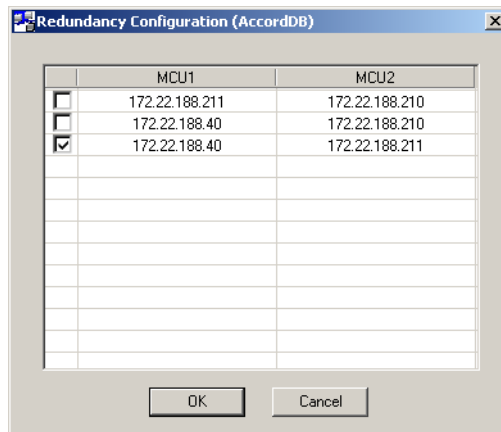
- The CDR files are separate on each MCU. A backup conference is identified by its prefix and when activated it will contain participants.



When MCU Redundancy is enabled, do not enter data in the field "User Defined 3" as it is reserved for the Central Server Service internal use.

MCU Redundancy Configuration

1. Click **Start-Programs > MGC Web Manager ver 9.0 > MGC Web Server Manager**.
The Login window is displayed.
2. Enter your *User Name* and *Password* and click **OK**.
MGC Web Server Manager window opens.
3. If required, add new MCUs to the list.
4. On the **Options** menu, click **Redundancy Configuration**.
The system displays a list of paired MCUs currently defined in the Web Server Manager.
5. Select the MCU pair(s) that you want to use to backup each other.



6. Click **OK**.
From this point on, all conferences, Meeting Room and Reservations will be mirrored between the MCUs in the select pairs.

MCU Backup

The Central Server Service enables you to schedule automatic system backup of selected MCUs. The automatic backup includes:

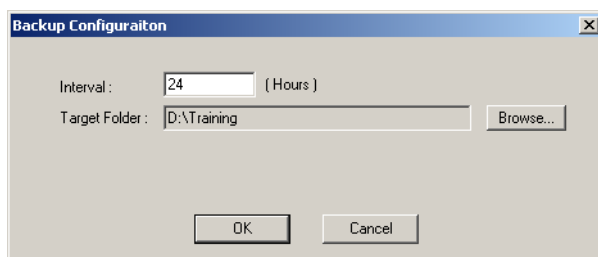
- System configuration (including Network Services and IVR Services)
- Meeting Rooms
- Reservations
- Conference Profiles
- Entry Queues

Defining the Backup Parameters

The backup interval and target path are defined once. It is important to connect the WebCommander Server and MCUs prior to the definition of the backup parameters as the first backup is performed when the definition is completed.

To define the Backup parameters:

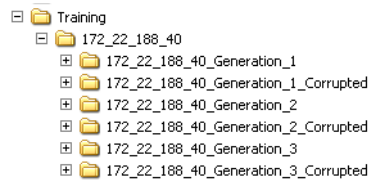
1. Click **Start-Programs > MGC Web Manager ver 9.0 > MGC Web Server Manager**.
The Login window is displayed.
2. Enter your *User Name* and *Password* and click **OK**.
MGC Web Server Manager window opens.
3. If required, right click the Server icon and then click **Connect Server**.
4. If required, add new MCUs to the list and connect them to the server.
5. On the **Options** menu, click **Backup Configuration**.
The Backup configuration dialog box is displayed.



6. Select the *Interval* in which the backups will be performed.
7. In the *Target Path*, click the **Browse** button to select the destination disk/folder where the backed up files will be stored.
8. Click **OK**.

The system automatically performs the first backup of all the connected MCU.

The information is saved to the selected target path (disk), creating a folder whose name is derived from the MCU IP address. For each backup, the system creates a folder with the suffix `_generation_n` where `n` is the backup number and in which the `dat`, `cfg` and `msg` folders are stored. If the backup fails for any reason (for example, if the MCUs are not connected or the WebCommander server is not active), the suffix `Corrupted` is added to the backup folder name in the format `_generation_n_corrupted`.



Version 9.0 Detailed Description - Secure Mode

You can configure the WebCommander application to be used in a Secure Mode. In Secure Mode all communications between the WebCommander components (WebCommander sites, WebCommander client, Server Manager application, OperServ, WAM and MCUs) are encrypted and authenticated.

The Secure Mode can be configured during the installation process or by switching the existing configuration from non-Secure Mode to Secure Mode.



The Personal Scheduler plug-in for Outlook that is used for scheduling conferences is disabled when working in Secured Mode as Personal Scheduler port is closed (default port is 5005).

Working in Secure Mode entails:

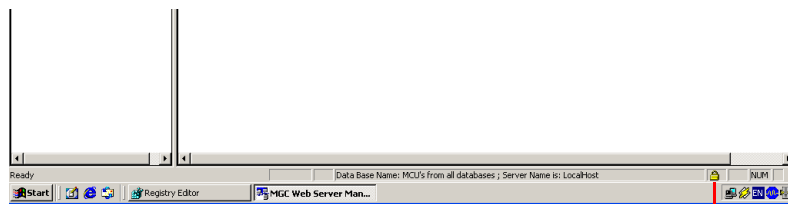
- All WebCommander sites are configured to work with SSL/TLS
- All WebCommander sites are configured to work only with "Integrated Windows Authentication"
- The Personal Scheduler application is disabled
- NT Authentication is required to access the Server Manager application
- All communication between application Server and MCUs is automatically secured
- MCU passwords in database are encrypted



The encryption of MCU passwords in the database depends on the operating system installed in the server:

- Windows 2003 Server implements AES encryption
- Windows NT and Windows 2000 implement 3DES encryption
- Adding MCUs and updating MCU passwords require a special permission

The Secure Mode is indicated by a lock icon that appears in the right corner of the Status bar of the Web Server Manager application.



Secure Mode indication

Secure Mode Prerequisites

Prior to setting the WebCommander to Secure mode, the MCU, IIS, SQL Database and DCOM must use secure encryption as follows:

- MCU - requires the installation of SSL/TLS certificate, setting the MCU port to Secured Port (port 443) and Secured mode and setting the appropriate system.cfg flags. For more information, see the MGC Administrator's Guide Chapter 2.
- Application Server (where the IIS, OperServ and WAM servers reside) - requires the installation of SSL/TLS certificate. This is done using the IIS. For more information, see "IIS Server - SSL/TLS Certificate Verification" on page 20.

- SQL Server (if using the SQL Database) - requires the installation of SSL/TLS certification and enabling the *Force Protocol Encryption* option. If the SQL Server is installed on the same server as the IIS (which is not recommended), only one SSL certificate is required (the one used for the IIS). For more information, see “Database Security Settings” on page 20.

IIS Server - SSL/TLS Certificate Verification

To ensure that the SSL/TLS certificate has been installed on the IIS:

9. Click **Start ->Settings ->Control Panel ->Administrative Tools ->Internet Information Services (IIS) Manager**.
The *Internet Information Services* window opens.
10. Expand the **Server name** list.
11. Right-click the **Default Web Site** icon and then click **Properties**.
The *Default Web Site Properties* dialog box opens.
12. Click the **Directory Security** tab, and then click **View Certificate**.
13. Verify that the system indicates that the certificate is valid.
14. Click OK and close the dialog box.

Database Security Settings

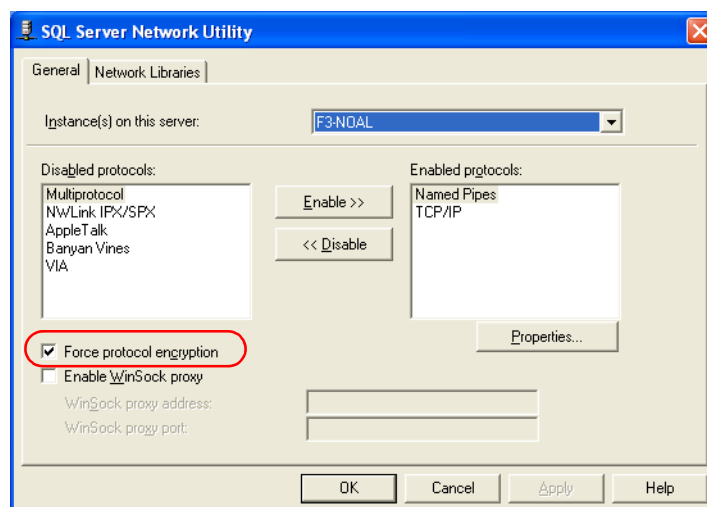
If an SQL database is used with the WebCommander, in addition to the installation of the SSL/TLS certificate, it must also be set to Secure Mode by selecting the Force Protocol Encryption option.

Enabling the Secure Mode:



When using an Access database or an external database the connection between WebCommander and the database is not secure.

1. On the *Start - Programs* menu, click **Microsoft SQL Server**, and then click **Server Network Utility**.
The *SQL Server Network Utility* dialog box opens.
2. Click the **Force protocol encryption** check box.



The connections to the SQL Server will be secured using SSL.

3. Click OK.

Secure Mode Implementation

The Secure Mode can be implemented in the WebCommander in the following ways:

- **New installation**

The following operations are performed:

- Selecting Secure Mode during the Installation of the WebCommander application. For more details, see “Installation Setup” on page 21.
- Verifying that the appropriate security settings were performed. For details, see “Verifying the Secure Mode Settings” on page 24.
- DCOM Config. For details, see “DCOM Configuration” on page 27.
- Set the working database as Global default so NT Authenticated users can be added to it Users table.
- It is recommended to set the default user Permissions to lower permissions and enable the permission add MCUs to the database or update the MCU passwords. All users that are automatically added to the WebCommander Users list will inherit this permission. For details, see “Permissions Setting” on page 33.

- **Upgrading an existing installation**

Install the new version in **non-secure** mode and then switch the installation to Secure Mode as described in "Switching a non-secured installation to Secure Mode"

- **Switching a non-secured installation to Secure Mode**

The following operations are performed:

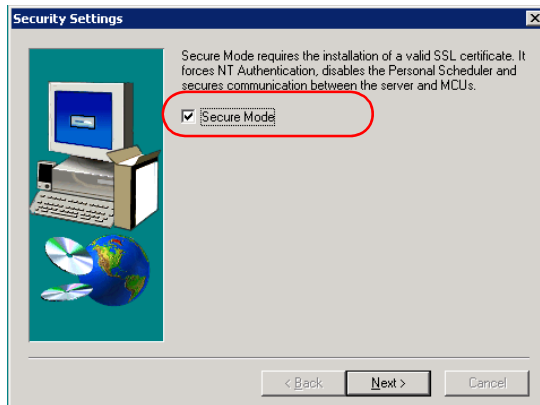
- In the Server Manager application, change the security settings in the *Web Configuration* dialog box. For details, see “Modifying the Security Settings in the Web Server Manager” on page 22.
- Verifying that the appropriate security settings were performed. For details, see “Verifying the Secure Mode Settings” on page 24.
- DCOM Config. For details, see “DCOM Configuration” on page 27.
- If instructed by the system, manually update the MCU passwords to encrypt them. For details, see “Manually Updating the MCU Password” on page 33.
- Set the working database as Global default so NT Authenticated users can be added to it Users table.
- It is recommended to set the default user Permissions to lower permissions and enable the permission add MCUs to the database or update the MCU passwords. All users that are automatically added to the WebCommander Users list will inherit this permission. For details, see “Permissions Setting” on page 33.

Installation Setup

When the Secure Mode option is selected during system installation, all the requires security configuration are automatically performed by the system.

This procedure should be performed only with new WebCommander installation. During the installation process, in the installation wizard:

- In the *Security Configuration* window, select **Secure Mode** and then click **Next**.



If you are upgrading from a non-secured installation, leave this check box cleared to install the new version in non-Secure Mode. Once the installation is complete, change the WebCommander security settings using the Server Manager application.

The *Information* dialog box opens indicating that the database must be configured to Secure Mode (if you have not done so prior to the WebCommander installation).

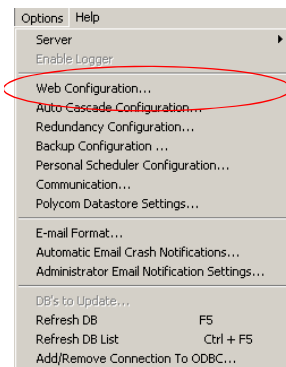
- Click **OK** to continue and complete the installation.

Modifying the Security Settings in the Web Server Manager

Perform this procedure to switch from non-Secure Mode to Secure Mode.

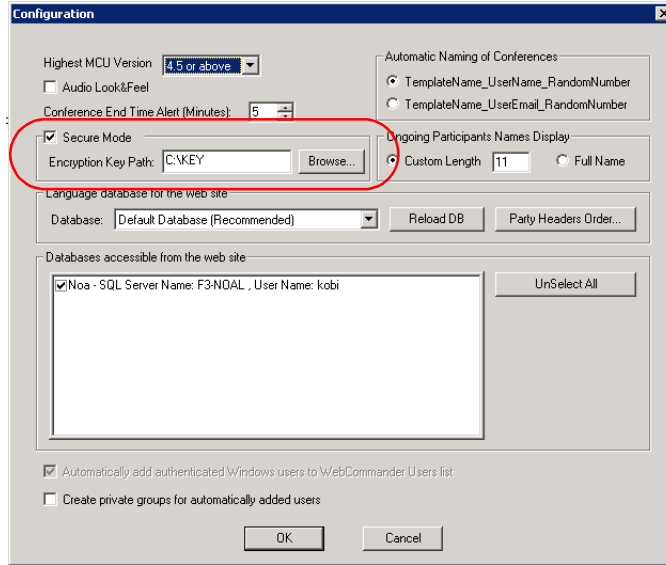
To enable the Secure Mode:

1. Access the **MGC Web Server Manager**.
2. On the *Options* menu, click **Web Configuration**.



The *Configuration* dialog box opens.

3. Click the **Secure Mode** check box.



Once you select this check box, the system displays a message listing the operations that will be performed when the WebCommander application is switched to Secure Mode.

4. Click **OK** to confirm. If you select **Cancel**, the system will clear the Secure Mode selection.
If OK is selected, the *Encryption Key Path* field is enabled and the *Automatically add authenticated Windows users to WebCommander Users list* option is automatically selected and cannot be cleared.
5. In the *Encryption Key Path* field, click the **Browse** button and select the folder to save the encryption key used to encrypt the MCU passwords in the database.
6. Click **OK**.

At this point, the system performs the following operations:

- Updates all the WebCommander sites (ConfSite, ConfpollerSite, WebCommander and Linked WebCommander) to work with SSL and integrated Windows authentication, while cancelling the anonymous access option.
- Encrypts the MCU passwords in the database.
If this operation fails, the MCU passwords must be manually re-entered to encrypt them.
- Stops and then starts the WebCommander services: Operserv, WAM and KeepAlive.
- Disconnects all the MCUs.
Once the system is restarted the MCU must be reconnected.
- This process takes about 10 seconds and at the end a confirmation message is displayed.

7. Click **OK**.
The system restarts and the user is automatically logged into the system.

Verifying the Secure Mode Settings

You can verify that the system performed the required changes in the security settings of the server and the OperServ by performing the procedures described next. These procedures are optional and can be skipped.

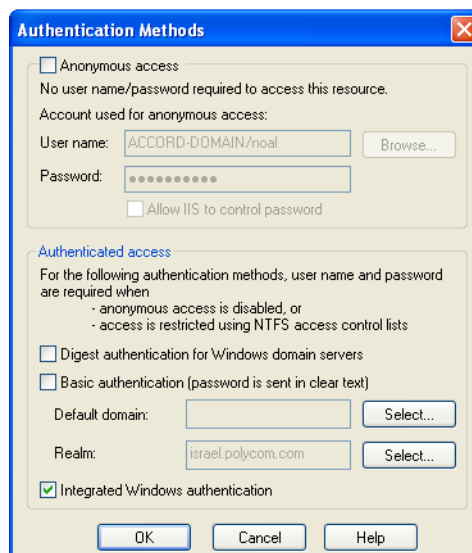
IIS Server Security Setting Verification

To ensure that the IIS Security Settings were enabled:

1. Click **Start ->Settings ->Control Panel ->Administrative Tools ->Internet Information Services (IIS) Manager**.

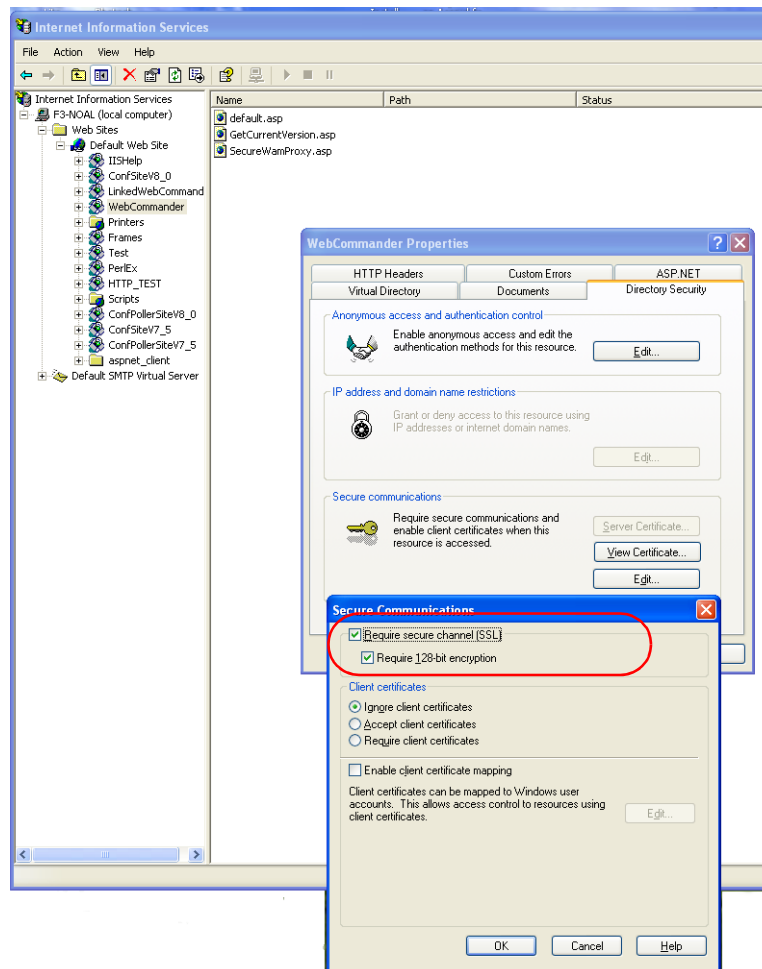
The *Internet Information Services* window opens.

2. Expand the **Server name** list.
3. Right-click the **Default Web Site** icon and then click **Properties**.
The *Default Web Site Properties* dialog box opens.
4. Click the **Directory Security** tab.
5. In the *Anonymous access and authentication control* box, click the **Edit** button.
6. Verify that the *Anonymous access* option is cleared and the *Integrated Windows authentication* option is selected and then click OK.



7. In the *Secure Communications* box, click the **Edit** button.
The *Secure Communications* dialog box opens.

8. Verify that the following check boxes are selected:
 - Require secure channel (SSL)
 - Require 128-bit encryption



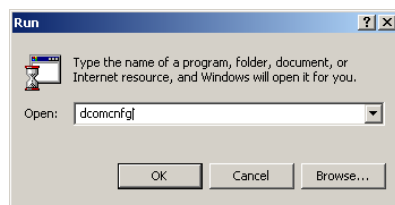
9. Click **OK** and then close the *WebCommander Properties* dialog box.

OperServ Security Settings Verification

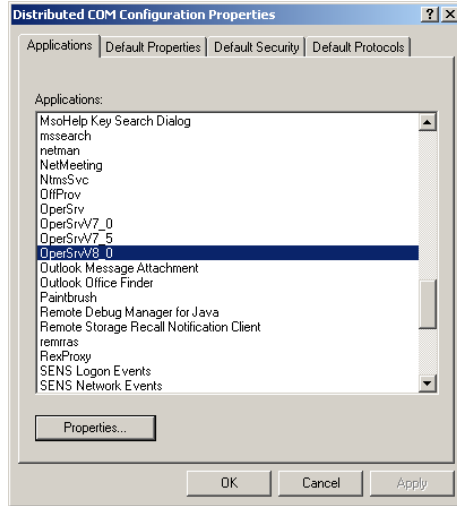
In Secure Mode, OperServ is set to the highest authentication level of *Packet Privacy*.

To verify the OperServ security settings:

1. Click **Start ->Run**.
The *Run* dialog box opens
2. In the *Open* field, type **dcomcfg** and click **OK**.

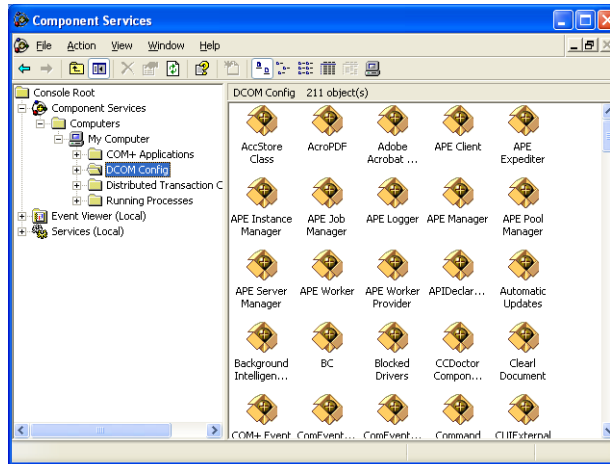


3. Access the OperServ properties.
 - a. In Windows 2000 server and Windows NT server, the *Distributed COM Configuration Properties* dialog box, click **OperServV9_0** and then click the **Properties** button.



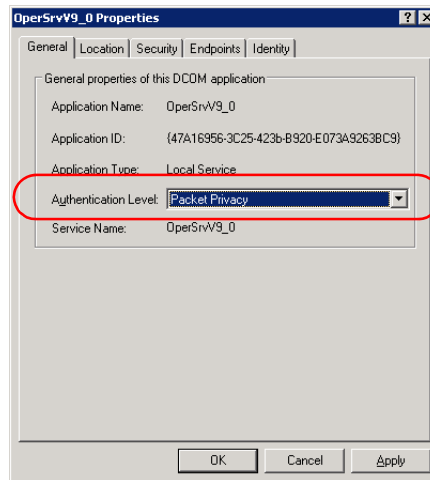
The *OperServ9_0 Properties - General* dialog box opens.

- b. In Windows XP server and Windows 2003 Server, in the *Component Services* window, click **Computers -> My Computer -> DCOM Config**.



- Right-click **OperServV9_0** and then click **Properties**.
The *OperServ9_0 Properties - General* dialog box opens.

4. Verify that **Packet Privacy** is selected in the *Authentication Level* field.



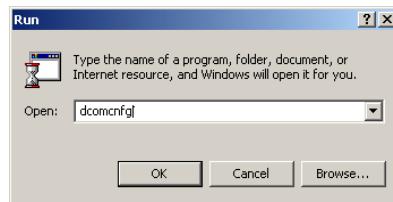
5. Click OK.

DCOM Configuration

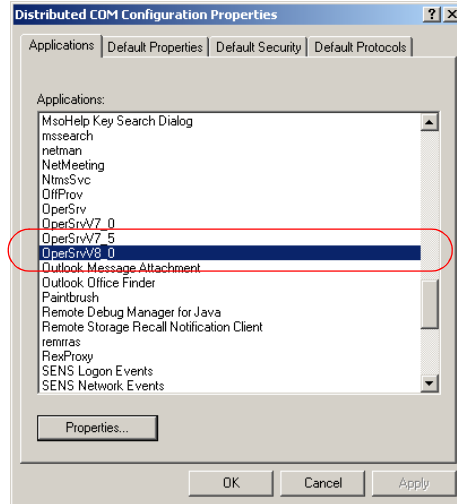
To grant various access rights to Windows authenticated users when using Web Server Manager Client and WebCommander Client, you must modify the properties of the OperServ and WAM services.

OperSrv Configuration for NT Authentication

1. Click **Start ->Run**.
The *Run* dialog box opens
2. In the *Open* field, type **dcomcnfg** and click **OK**.

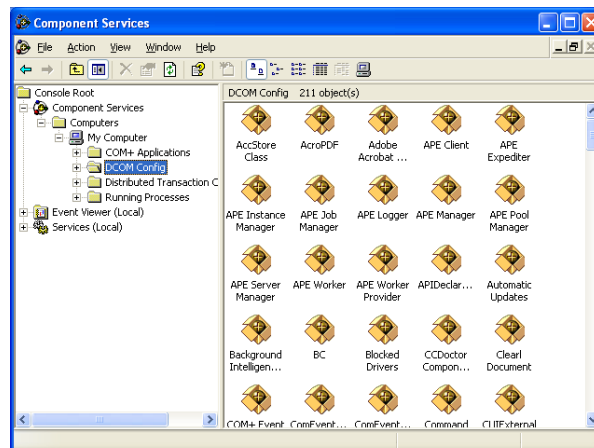


3. Access the OperServ properties.
 - a. In Windows 2000 server and Windows NT server, the *Distributed COM Configuration Properties* dialog box, click **OperServV9_0** and then click the **Properties** button.



The *OperServ9_0 Properties - General* dialog box opens.

- b. In Windows XP server and Windows 2003 Server, in the *Component Services* window, click **Computers -> My Computer -> DCOM Config**.

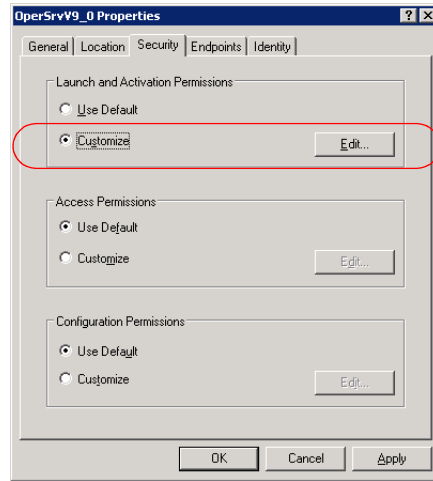


- Right-click **OperServV9_0** and then click **Properties**.

The *OperServ9_0 Properties - General* dialog box opens.

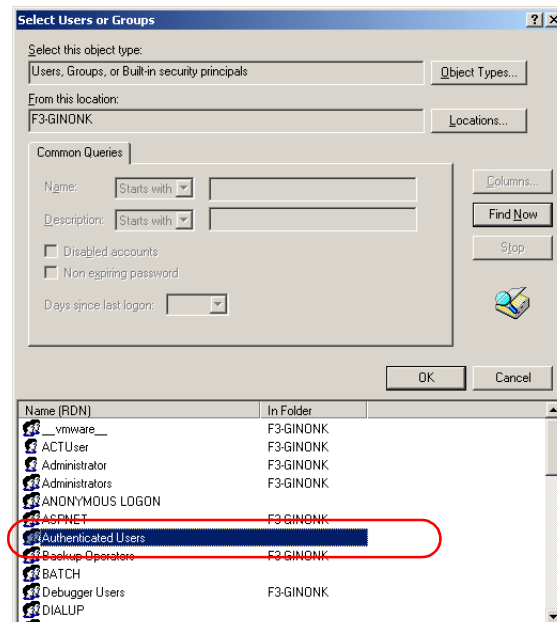
4. Click the **Security** tab.

- In the *Launch and Activation Permissions* pane, select **Customize** and then click the **Edit** button.



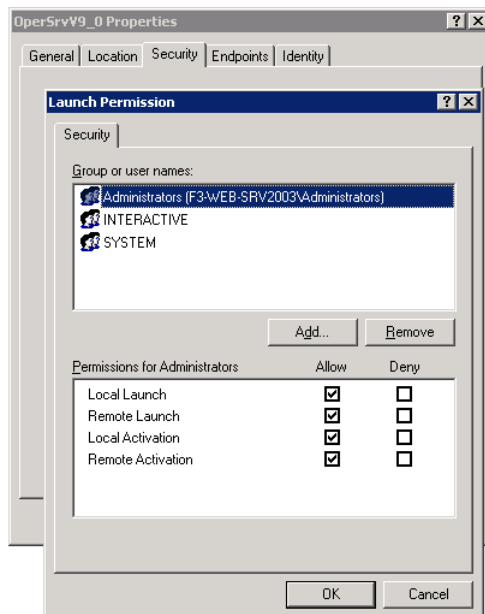
The *Launch Permission* dialog box opens.

- Click the **Add** button.
The *Select Users, Computers or Groups* dialog box opens.
- Click the **Locations** button.
The *Locations* dialog box opens.
- Select the local computer name.
- Click the **Advanced** button.
- Click the **Find Now** button.
A list of users is displayed.
- Select the **Authenticated Users** group and click **OK**.



The selected Group is added to the *Launch Permission* dialog box, in the *Group or user names* list.

12. Set the permission to **Allow - Local launch, Allow - Local Activation, Allow - Remote Launch** and **Allow - Remote Activation**.



13. Click **OK**.
14. In the *Security* tab, set *Access Permission* to **Customize** and click the **Edit** button.
15. Repeat steps 6 to 13 performed for *Launch Permission* also for *Access Permission*.
16. At the end of the procedure, click **OK** to close the *Properties* dialog box.

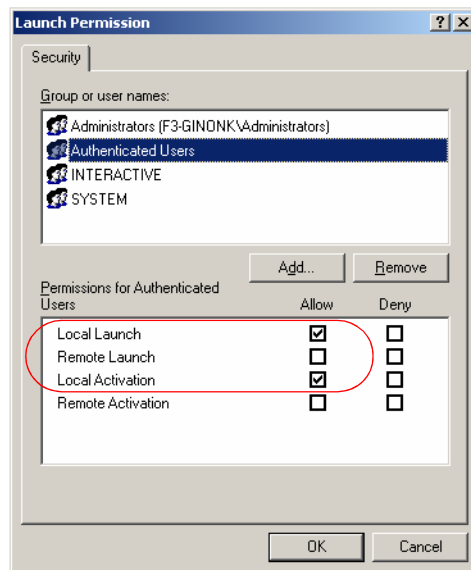


Do not close the *Distributed COM Configuration Properties* dialog box (Windows NT) or the *Component Services* window, in which the DCOM Config services are listed as you will need it for the next procedure.

WAM Configuration for NT Authentication

1. Access the WAM properties.
 - a. In Windows 2000 server and Windows NT server, the *Distributed COM Configuration Properties* dialog box, click **WAM** and then click the **Properties** button.
The *WAM Properties - General* dialog box opens.
 - b. In Windows XP server and Windows 2003 server, in the *Component Services - DCOM Config* list, right-click **WAM** and then click **Properties**.
The *WAM Properties - General* dialog box opens.
2. Click the **Security** tab.
3. Repeat steps 5 to 11 in the "OperSrv Configuration for NT Authentication" procedure.

- In the *Permissions for Authenticated Users* pane, set the permission to **Allow - Local Launch** and **Allow - Local Activation**.



- Click **OK** to close the *Properties* dialog box.

Allowing Connecting/Starting the Application Server (OperSrv) from Server Manager Clients

Windows 2003 server

- In the server computer, right-click the **My Computer** icon and then click **Manage**.
- Expand the **System Tools** tree.
- Expand the **Local Users and Groups** tree
- Click the **Groups** folder to display its list.
- Right-click the **Distributed COM Users** group and click **Properties**.



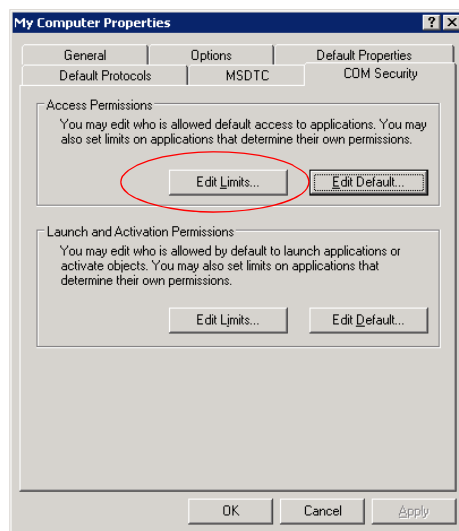
The "Distributed COM Users" group exists only from Windows 2003 server. For Windows NT server and Windows 2000 server, it is recommended to create a new domain's user group for remote Server Manager Clients, and add the group once to the Groups list instead of adding users one by one. For more details, see "Creating a Group and granting permissions to the group in Windows NT server and Windows 2000 server" on page 32.

- Click the **Add** button.
The *Select Users, Computers or Groups* dialog box opens.
- and add the user or users' group to this group.
- Click the **Locations** button.
The *Locations* dialog box opens.
- Select the local computer name.
- Click the **Advanced** button.
- Click the **Find Now** button.
A list of users is displayed.

12. Select the **Authenticated Users** group and click **OK**.
The selected Group is added to the *Distributed COM Users* group in the *Group or user names* list.
13. Click **OK**.

Creating a Group and granting permissions to the group in Windows NT server and Windows 2000 server

1. In the server computer, right-click the **My Computer** icon and then click **Manage**.
2. Expand the **System Tools** tree.
3. Expand the **Local Users and Groups** tree
4. Right-click **Groups** folder and then click **New Group**.
The *New Group* dialog box opens.
5. Click the **Add** button and add the required users to this group.
6. Click **OK**.
7. Click **Start ->Run**.
The *Run* dialog box opens
8. In the *Open* field, type **dcomcfg** and click **OK**.
9. In the *Component Services* window, expand the **Computers** list.
10. Right-click **My Computer** and then click **Properties**.
11. Click the **COM Security** tab.
12. In the *Access Permissions* box, click the **Edit Limits** button.



The *Access Permission* dialog box opens.

13. Click the **Add** button and add the group you have created to the list.
14. Set the group permissions to **Allow - Local Access** and **Allow - Remote Access**.
15. Click **OK**.
You are returned to the *COM Security* tab.
16. In the Launch and activation Permissions box, click the **Edit Limits** button.
17. Click the **Add** button and add the group you have created to the list.

18. Set the group permissions to **Allow - Local Access**, **Allow - Remote Access**, **Allow - Local Activation**, and **Allow - Remote Activation**.
19. Click OK.

Manually Updating the MCU Password

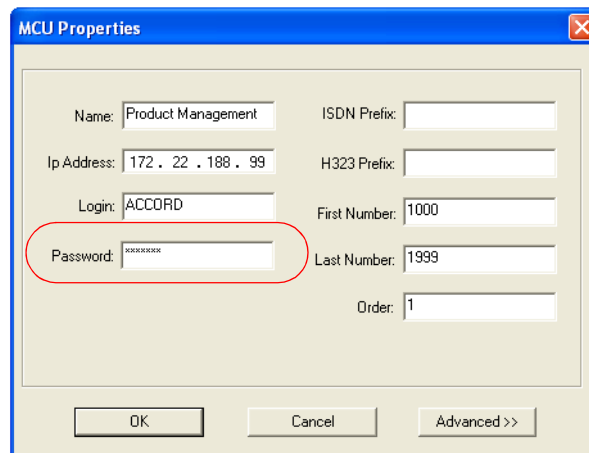
This procedure must be performed when:

- You have selected the Secure Mode option during the installation of version upgrade. In such a case, passwords of MCU already defined in the database are not encrypted automatically and they must be re-entered to encrypt them.
- The system failed to automatically update the MCU passwords when switching to Secure Mode.

When adding or changing MCU passwords in Secure Mode, they are automatically encrypted by the OperSrv and stored in the database.

To re-enter the MCU password:

1. In the *Web Server Manager*, expand the SQL database tree and click **MCU's**. The list of MCU's appears.
2. For each MCU in the MCU list, right-click the MCU icon and click **Properties**. The MCU Properties dialog box appears.
3. In the *Password* field, re-enter the password. The password is hidden by a series of asterisks (*****).



4. Click OK.

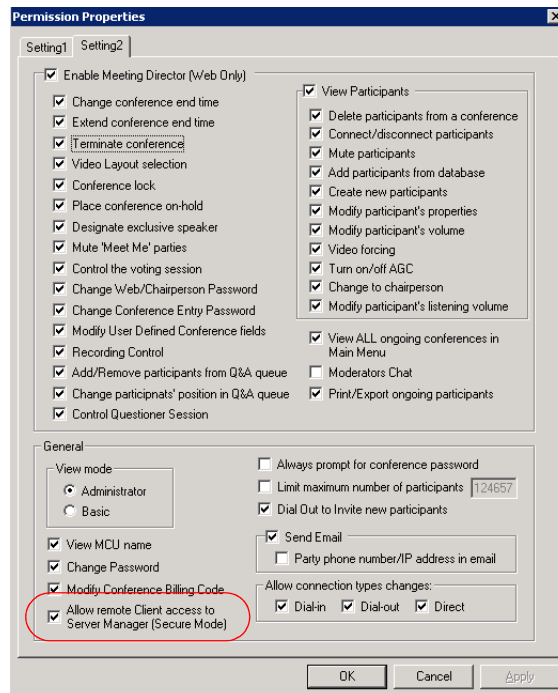
Permissions Setting

Any NT Authenticated user that is added to the WebCommander users list is automatically given default user's permission. When adding an MCU to the database or when modifying the MCU password in Secure Mode, the user must have a special permission to perform these operations.

To grant permission:

1. In the *Web Server Manager*, expand the *Database* tree and click **Permissions**. The *Permission Properties* dialog box opens.

2. Click the **Settings2** tab.
3. Click the **Allow remote Client access to Server Manager (Secure Mode)** check box.



4. Click **OK**.

Switching from Secure Mode to Non-Secure Mode

When reverting back to a non-secure mode, the following operations are performed:

- In the Server Manager application, in the Web Configuration dialog box, clear the Secure Mode check box.

The system displays a message indicating the process that will be performed once the operation is confirmed.

These operations include:

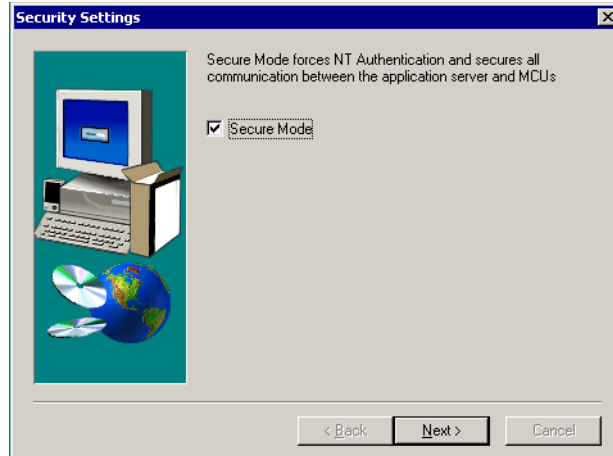
- Restoring the IIS defaults (turning off SSL/TLS and NTLM Authentication, and turning on Anonymous access)
- Restarting all the WebCommander services
- Enabling the Personal Scheduler application
- Decrypting MCU passwords in ALL connected databases
- Once the process is complete, the Login dialog box is displayed and the user must enter the User Name and Password.

WebCommander Server Client Installation

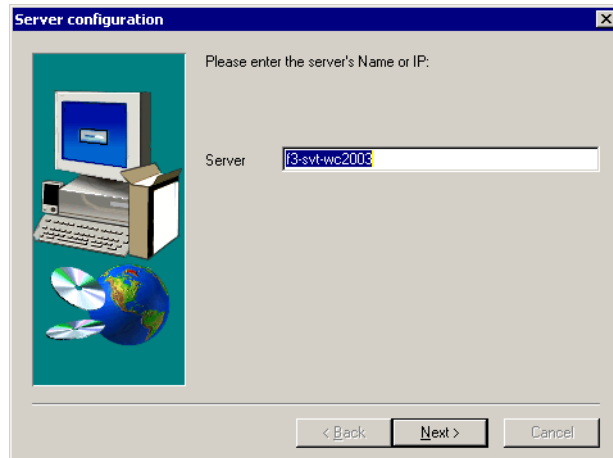
WebCommander Server client installations cannot be switched from non-Secure Mode to Secure Mode and vice versa and must be re-installed.

To install the WebCommander Server Client in Secure Mode:

- In the installation setup procedure, select the **Secure Mode** option.



- Select the name or IP of the WebCommander server. The server name must be identical to name for which the SSL/TLS certificate was issued (and installed on the server).



Version 9.0 - Corrections, Limitations and Pending Issues

Version 9.0 Corrections

Corrections between Versions 8.0 and 9.0

Table 1: Corrections between 8.0 and 9.0

#.	Subject	Description	ID#	Remarks
1.	Web Server Manager	In the Web Server Manager there is no indication that the Central Server Service is down.	VNGM-1894	
2.	Personal Scheduler	When the German language is selected, the Invite dial-out endpoints window appears in English.	VNGFE-701	
3.	Automatic Discovery Mode	When connecting an MCU to the server using port 443 and the Automatic Discovery Mode mode is enabled, if the OperSrv Service is restarted, the MCU fails to connect.	VNGFE-655	
4.	WebCommander	WebCommander cannot display the conference list when participant names include quotation marks.	VNGFE-804	

Corrections between Versions 7.5 and 8.0

Table 2: Corrections between 7.5 and 8.0

#.	Subject	Description	ID#	Remarks
1.	E-mail Notification	In the email notification of a recurrent reservation the conference Numeric ID is missing.	22388	
2.	E-mail Notification	When using Microsoft Outlook to modify the time of a meeting in recurring reservations, there is no text in the message body of the sender mail. This occurs whether a single occurrence is updated or the whole series. This occurs with WebCommander Server version 7.01.10 and PS Client V.7.0.1.5.	22389	

Table 2: Corrections between 7.5 and 8.0

#.	Subject	Description	ID#	Remarks
3.	Personal Scheduler	The monitor link in the New Meeting request is incorrect and does not include the DNS server name as it is configured in the Server Manager.	22497	
4.	External Database	External Database Authentication does not work with MCU version 7.5.0.52 and WebCommander version 7.5.0.13.	22396	
5.	Web Server Manager	When attempting to define the Administrator Send Email Configuration option in the Web Server Manager application, in error message is displayed: "Unsupported operation".	22498	
6.	WebCommander	After server reboot, the MGC unit and the Web Server do not connect automatically.	22454, 22404	
7.	WebCommander	WebCommander version 7.5.1.1 does not accept any version 7.0 License key.	22572, 22966	
8.	WebCommander	With WebCommander versions 7.0 and 7.5, when working with MGC Manager version 7.02.6 and scheduling a conference or a Reservation with FECC/LSD, an error message is displayed: "Failed to Start reservation".	22878	
9.	Windows	Manually stopping the Opersrv Service in Windows Enterprise Manager results in error messages: "Could not stop the OperSrvV7_5 service on local Computer", and " Error 1067: The process terminated unexpectedly".	22496	

Version 9.0 System Limitations

Table 3: System Limitations

No.	Subject	Description	ID#	Workaround/Remarks
1.	Double Booking	When making a conference reservation for today and selecting a future date for the recurrent reservation, the Double Booking window appears for today's booking.	14742	
2.	Email Notification	When customizing the format of the Email (in any language), there is no default format.	16014	
3.	E-mail Notification	When the <i>From</i> field in an e-mail is not filled in, the system does not display a warning message.		
4.	On Going Conference	When the system cannot support the Exclusive Speaker mode due to the incorrect card type, a status message does not appear.	14650	
5.	Permissions	If the conference organizer does not have permission to change user settings, any passwords the organizer configures will be ignored and the conference will start with passwords defined by the MCU.		
6.	Personal Scheduler	In the MGC Manager, when printing the parameters of a Continuous Presence conference scheduled from the Personal Scheduler, the layout of 1x1 appears as "unknown" in the printed data.	11812	
7.	Personal Scheduler Server	When configuring the Personal Scheduler Server (after installation), the Language drop-down list appears empty.	14676	Click the arrow to display the list of languages and select the appropriate language.
8.	Personal Scheduler Client	Personal Scheduler Clients version 5.6 cannot connect to Personal Scheduler server version 6.0.	13607	backward compatibility is enabled from Version 7.0
9.	Personal Scheduler Client	When creating a recurrent reservation "on behalf" of a colleague, the conference IDs for the recurring reservations are incorrect.	15264	
10.	Personal Scheduler Client	Personal Scheduler version 5.6 and Personal Scheduler version 6.0 should not be installed on the same server as version 6.0 is not backward compatible with previous Personal Scheduler versions.	13640	

Table 3: System Limitations

No.	Subject	Description	ID#	Workaround/ Remarks
11.	Recurrent reservation	In WebCommander, after changing the start time of a single recurrent meeting using Drag & Drop, if you try to update the entire series, an error message is displayed: "Operation failed".	18007	
12.	Reservation Calendar	The name of the MCU cannot contain an apostrophe ('), otherwise a Java script error occurs.		
13.	Reservation Calendar	After updating a recurring reservation in Outlook 2003 and sending an update by e-mail, the invitee receives an email with a "Polycom Office" tab.	18390	
14.	Reservation templates	When setting up an Entry Queue access conference, the Continuous Presence - Quad View option is enabled.		
15.	Reservation templates	If you change the layout colors of the conference and start the conference, the colors will revert to the default colors after the conference is over, even if you save the template.		You must change the layout colors before the start of each conference.
16.	Screen Resolution	You are unable to view the WebCommander GUI if your screen resolution exceeds 600x800.	13733	
17.	Server Manager	In the Server Manager, when modifying the name of an existing Default Reservation set from lower case to upper case, the system indicates that the default reservation set already exists.	14860	
18.	Version Upgrade	When upgrading WebCommander version 6.0x installed with PathNavigator database and NT Authentication to WebCommander version 7.0 using the PathNavigator database with SQL Authentication, the PathNavigator database is not added or connected to the WebCommander database list.	18999	Update the database list using NT Authentication.

Pending Issues Version 9.0

Table 4: Pending Issues

#.	Subject	Description	ID#	Remarks
1.	Personal Scheduler Client	In the "Polycom office" tab, the field "Dial-in Endpoints/Phones" appears in all types of conferences. This field should appear only in "Entry Queue" or "Meet-Me per" conferences.	17887	
2.	Personal Scheduler Client	A viaVideo auto connection is not supported when the system.cfg flag 'Quick login Via EQ' is set to YES.	18713	Create a regular conference and check the 'Enable numeric conference name' checkbox in the 'MGC Personal Scheduler Configuration'. For reservation recurrences, use EQ Access or Entry Queues to solve the problem.
3.	Personal Scheduler Reservation	Create a recurring reservation, then click Edit, and then change the subject name. The name does not change.	18374	
4.	Recurrent Reservation	As the recurrent reservation's Name field is limited to 73 characters, using long names may result in missing characters since WebCommander automatically adds the user-name and numbers to each reservation occurrence.	17829	Reservation names should be shorter than 50-60 characters.
5.	Recurrent Reservation	When user A creates a single recurring meeting on behalf of user B, when user B updates the meeting, user A cannot re-open the meeting on behalf of user B.	19268	
6.	Reservation Calendar	After an update of recurrence fails, it is impossible to access any recurring reservation.	18010	
7.	Reservation Calendar	When editing a recurrent meeting, the reservations are deleted and recreated with the changes. If the number of recurrent reservations is large, it takes a long period of time to generate and process.	18373	

Table 4: Pending Issues

#.	Subject	Description	ID#	Remarks
8.	Reservation Default	When you copy and paste the Reservation Default template from one database to another, some parameters are copied incorrectly.		The fields that were not copied correctly must be changed manually. The fields are: Interlaced Video Mode, Dual Stream Mode, Conference on Port, Entry Queue Access, Meet Me Per Conference, Meeting Room, Start Conference Requires Chairperson, Terminate After Chairperson Exits, On Hold, Invite Party, Background, Layout Border, Speaker Notation.
9.	Reservations in Japanese or Chinese	When using WebCommander in Japanese or Chinese languages, the confirmation button to schedule new conferences is missing from the <i>New Meeting</i> page.		You must schedule the reservation from the Reservations Templates window.

Proprietary and Confidential

The information contained herein is the sole intellectual property of Polycom, Inc. No distribution, reproduction or unauthorized use of these materials is permitted without the expressed written consent of Polycom, Inc. Information contained herein is subject to change without notice and does not represent commitment of any type on the part of Polycom, Inc. Polycom and Accord are registered trademarks of Polycom, Inc.