297-2183-117

Nortel Networks Symposium Call Center Web Client

Planning, Installation, and Administration Guide

Product release 4.5 Standard 1.0 July 2003

NORTEL NETWORKS™


Customer Contact Web.com
Member's Choice
AWARD
2002
Winner


Call Center &
CRM Solutions
2002
Best
of Show
CUSTOMER interface


PRODUCT
CUSTOMER INTERACTION Solutions
2002
OF THE YEAR


2002
TMC
Communications
SOLUTIONS
Product Of The Year

Nortel Networks Symposium Call Center Web Client

Planning, Installation, and Administration Guide

Publication number:	297-2183-117
Product release:	4.5
Document release:	Standard 1.0
Date:	July 2003

Publication history

July 2003

The Standard 1.0 version of the *Nortel Networks Symposium Call Center Web Client Planning, Installation, and Administration Guide*, Release 4.5, is released.

Contents

1 Getting started 11

Overview 12
About Symposium Web Client 15
Skills you need 24
Related documents 25
System requirements 26
Disk partitions and communication ports 41
Symposium Web Client and Crystal Reports 44

2 Preparing Symposium Call Center Server 47

Overview 48
Modifying Real-time Statistics Multicast settings 49
Testing the Real-time Statistics Multicast service 58

3 Installing and configuring application server software 61

Overview 62

Section A: Windows 2000 server 63

Overview 64
Symposium Web Client and replication 65
Windows 2000 Server/Advanced Server installation and configuration 67
Applying security patches to the application server 70

Section B: Installing third-party software on the application server 73

Overview 74
Installing Microsoft Active Directory 75
Installing Sybase Open Client on the application server 88

Section C: Installing Symposium Web Client on the application server 95

Overview 96
Installing Symposium Web Client on the application server 98
Installing or repairing individual Symposium Web Client components on the application server 116
Uninstalling application server software 122

Configuring multiple-language support 128
Configuring multiple language support in Agent Desktop Displays 143

Section D: Backing up and restoring user data 145
Overview. 146
Backing up Symposium Web Client data. 148
Restoring Symposium Web Client data 153
Replication considerations 161

Section E: Configuring the application server 163
Overview. 164
Configuring Real-Time Reporting 165
Configuring Emergency Help. 173
Configuring Historical Reporting. 175
Configuring Scripting 183
Configuring Agent Desktop Displays. 194

Section F: Security and the application server 197
Overview. 198
Removing the Everyone group from the application server. 200
Installing, configuring, and uninstalling IIS Lockdown and URLScan 207
Changing the default anonymous Internet Guest account 248
Disabling the parent path in IIS 263
Enabling Secure Sockets Layer on the application server 266
Configuring Terminal Services in a secure environment 271

4 Installing and configuring client software 287
Installing third-party software on a client. 288
Installing and configuring Agent Desktop Displays on a client PC 320

5 Upgrading Symposium Web Client 333
Overview. 334
Pre-upgrade checklist 335
Upgrading Symposium Web Client 338
Upgrading the Agent Desktop Displays client software. 352
Applying the latest Service Update 363

6 Using Symposium Web Client 369
Overview. 370

Section A: Getting started with Symposium Web Client 373
Overview. 374
High-level task flow 375
Starting Symposium Web Client 378

Section B: Configuration 383
Overview. 384
Adding and configuring call center servers 386
Configuring resources. 391

Section C: Contact Center Management 401
Overview. 402
Working in supervisor view 404
Working in agent view 408
Working in skillset view. 414
Working in assignments view. 417
Adding Symposium Call Center Server users 420
Using the XML automated assignments feature. 426

Section D: Access and Partition Management 435
Overview. 436
Creating report groups 441
Creating partitions. 444
Creating access classes 453
Adding and configuring users. 462
Supervisor/reporting agents feature 464

Section E: Audit Trail 481
Overview. 482
Monitored resources 484

Section F: Scripting 487
Overview. 488
Viewing scripts 489
Creating and editing scripts 490
Validating your script 492
Displaying script variables and parameters 493
Viewing, editing, and assigning application threshold classes. 495
Working with sample scripts 497
Checking variables for referencing scripts 499

7 Troubleshooting 501
Technical support 502
Client PC. 507

Application server. 517
Simple Object Access Protocol errors 531

A Installation worksheets and checklists 535
Overview. 536
Pre-installation worksheet. 537
Installation checklist 545
Windows 2000 Server/Advanced Server installation checklist 550

B IP Multicast Networking 559
Overview. 560
Multicast sending and receiving 561
Implementing IP multicasting for Symposium Web Client 571

C Web site types 575
Determining your web site type 576

D Third-party controls required on the client PC 579
Third-party controls 580

E Supervisor/reporting agents matrix 583
Overview. 584
Real-Time Reporting 585
Historical Reporting 591
Contact Center Management 593

Glossary 595

Index 621

Chapter 1

Getting started

In this chapter

Overview 12

About Symposium Web Client 15

Skills you need 24

Related documents 25

System requirements 26

Disk partitions and communication ports 41

Symposium Web Client and Crystal Reports 44

Overview

Introduction

The *Symposium Call Center Web Client Planning, Installation, and Administration Guide* provides step-by-step instructions for the procedures you must perform to complete the installation and administration of Symposium Web Client.

For tips on installing the Symposium Web Client and operating system software, see Appendix A, “Installation worksheets and checklists.” These checklists include tips on installing the following third-party software:

- Windows 2000 Advanced Server or Windows 2000 Server with Service Pack 3 (minimum), Service Pack 4 or later (recommended) with Terminal Services, and Internet Information Services (IIS), on the Symposium Web Client application server

Note: As Service Packs for Windows 2000 become available, Nortel Networks tests them for compatibility against the Symposium Web Client software as soon as possible. Nortel Networks recommends that customers upgrade to new service packs as per vendor (Microsoft) recommendations, because critical service packs may include security enhancements.

See Chapter 3, “Installing and configuring application server software” for details on installing the following software:

- installing Microsoft Active Directory
- configuring Terminal Services, Terminal Services Licensing, and Simple Mail Transfer Protocol for Symposium Web Client
- installing Symposium Web Client on the application server
- installing third-party applications, such as Sybase Open Client
- uninstalling Symposium Web Client or one of its components on the application server

Note: The Symposium Web Client installation includes some Crystal Reports 9.0 components that are required for running reports. The installation does *not* include the full, report-writing version of Crystal Reports. For more information, see “Symposium Web Client and Crystal Reports” on page 44.

For details on installing software on the client PCs, see Chapter 4, “Installing and configuring client software.” This chapter includes the procedure for installing the following software:

- Agent Desktop Displays client

Who should read this guide

This guide is intended for

- Nortel Networks installers and distributors who are responsible for installing Symposium Web Client
- administrators who are responsible for monitoring and maintaining the application server

Access rights

This guide assumes that you have the privileges and access rights required to perform the procedures in this guide.

ATTENTION

When you install Symposium Web Client, the Web Client setup wizard creates a Windows 2000 Server/Advanced Server user called *iceadmin* and assigns full administrative access rights to this user. If you delete this user or modify the user’s password in Windows 2000 Server/Advanced Server after you install the Symposium Web Client software, then you will not be able to log on to Symposium Web Client either as *webadmin*, or any other user. You must not change the *iceadmin* password after you install the software.

Key codes

Nortel Networks supplies a special code called a key code that you need to enter during the installation. This key code gives you access to all of the Symposium Web Client components.

About Symposium Web Client

What is Symposium Web Client?

Symposium Web Client is a browser-based tool for call center administrators and supervisors. You can use Symposium Web Client to manage and configure a call center and its users, define access to data, and view real-time and historical reports.

Symposium Web Client provides these functions with the following components:

- Contact Center Management
- Access and Partition Management
- Configuration
- Scripting
- Real-Time Reporting
- Historical Reporting
- Emergency Help
- Audit Trail
- Agent Desktop Displays

Symposium Web Client components

Contact Center Management

Use Contact Center Management to add, edit, view, or delete

- users (agents, supervisors, or supervisor/agents) on a server in Symposium Call Center Server
- agent to supervisor assignments
- agent to skillset assignments

Access and Partition Management

Use Access and Partition Management to add, edit, view, or delete

- Symposium Web Client users
- partitions
- access classes
- report groups for Historical Reporting
- basic access rights to different Symposium Web Client components

You also use this component to assign access classes, partitions, and supervisor/reporting agent combinations to Web Client users.

When you add a user in Access and Partition Management, you add a Web Client user. Web Client users can log on to the application server and use the Symposium Web Client components to which they have been given access. To add a user (agent, supervisor, or supervisor/agent) to Symposium Call Center Server, you must use the Contact Center Management component, or use the spreadsheet in the Configuration component.

Note: Some Symposium Call Center Server users (supervisors and supervisor/agents) may also be Web Client users and be given a Web Client user ID and password to access the application server; however, many Symposium Call Center Server users will never use Symposium Web Client.

Configuration

The Configuration component assists you in configuring and administering Symposium Call Center Server. You can also download a preformatted Excel spreadsheet from the Configuration component to upload and download Symposium Call Center Server configuration and user information.

Note: You can use the M1 Data Extraction Tool to extract configuration data from the M1, and then upload that data to Symposium Call Center Server by using Symposium Web Client's Configuration spreadsheets. For more information, refer to the *Symposium Call Center Web Client Data Extraction Tool User's Guide for the Meridian 1*. The M1 Data Extraction Tool is intended for use with the M1 switch only; it may not support the Meridian 1 Internet Enabled switch.

The Configuration component of Symposium Web Client is also available separately as a stand-alone application called the Symposium Configuration Tool.

Note: If you are on site configuring a customer's call center, you can upload your Symposium Configuration spreadsheets using the Configuration component of the customer's Symposium Web Client application.

Scripting

Symposium Call Center Server uses scripts to route calls. With the Scripting component, you can create and modify call routing instructions for your call center using the following components:

- a Script Manager
- a Script Editor
- a Script Variable creator
- a Script Command Reference

You can also apply thresholds to your applications, and edit application threshold classes using the Scripting component.

The Scripting component also includes a validation tool that checks your scripts for errors before they run.

Real-Time Reporting

Use the Real-Time Reporting component to view the dynamics of call activity. Real-time displays are available for both networked and single sites. The following standard Real-Time Reporting displays are available in Symposium Web Client:

- six nodal real-time displays for single Symposium Call Center Server sites
- three network-consolidated real-time displays for a network of Symposium Call Center Server sites

Historical Reporting

Use Historical Reporting to gather information about the past performance of the call center. You can generate two types of historical reports:

- Summarized historical reports contain totals for information gathered during a specific interval of time (for example, daily totals or weekly totals).
- Event/detail reports are detailed reports for specific events that have occurred in the call center (for example, an Agent Activity report).

Emergency Help

When a supervisor opens the Emergency Help panel, the system notifies the supervisor automatically whenever an agent presses the Emergency key on his or her phoneset. Agents can press the Emergency key when they require assistance from the supervisor (for example, if the caller is abusive). The Emergency Help panel shows information about the agent, including the agent's name, location, and time when the Emergency key was pressed.

Audit Trail

Audit Trail records the actions performed in the Configuration component, and identifies the user ID of the person who made the changes.

Symposium Agent Desktop Displays

Symposium Agent Desktop Displays provides real-time skillset monitoring to agents. Agent Desktop Displays must be configured on the application server, and on client PCs that use the tool.

The network components of Symposium Web Client

Symposium Web Client uses a three-tiered Internet-based architecture with functionality distributed among various components. The major components of Symposium Web Client include the following:

Symposium Web Client client PCs—Employ a web-based browser to interface with the application server. They are used to administer the server and to monitor call center performance.

Symposium Web Client application server—The middle layer that communicates with Symposium Call Center Server and makes information available to the client PCs.

Symposium Call Center Server—Responsible for functions such as the logic for call processing, call treatment, call handling, call presentation, and the accumulation of data into historical and real-time databases.

Network considerations

This section outlines some considerations you must make when running Symposium Web Client in either of the following network configurations:

- **single node Symposium Call Center Server** In this configuration, each application server is paired with a single server in Symposium Call Center Server.
- **multiple servers in Symposium Call Center Server** In this configuration, each application server can be configured to manage multiple servers in Symposium Call Center Server simultaneously.

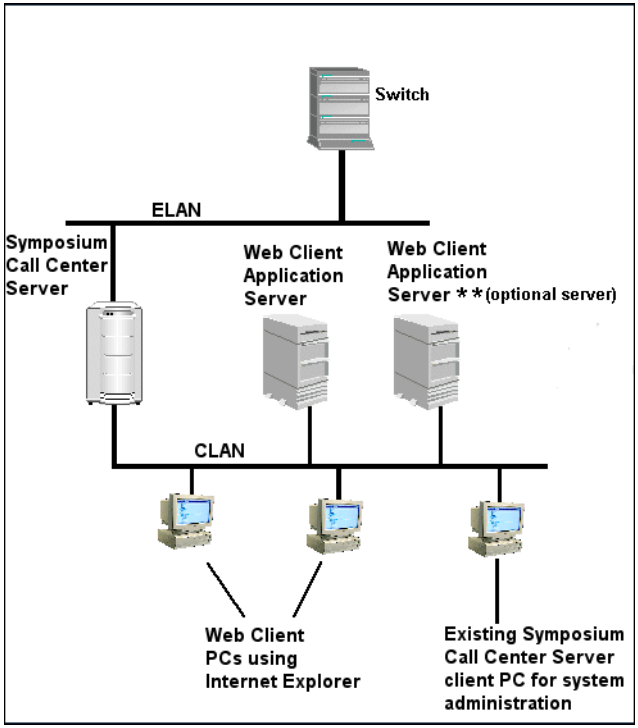
Single node Symposium Call Center Server

Typically, in a single node environment, one Symposium Web Client application server is paired with the server in Symposium Call Center Server; however, more than one application server can be paired with the server in Symposium Call Center Server (you may want to implement more than one application server for load balancing, redundancy, and so on).

If more than one application server is used, each application server must be configured as a stand-alone application server (for example, different send multicast IP addresses). Each Symposium Web Client application server acts as the consolidation point for real-time data from its paired server in Symposium Call Center Server. Multiple application servers can share the same user data (user preferences) by using Active Directory replication. For details on replication, and the limitations on data sharing, see “Symposium Web Client and replication” on page 65.

The following diagram depicts this type of configuration:

Single node Symposium Call Center Server



Considerations and decision criteria

Note the following when deciding whether to configure Symposium Web Client in a single node environment.

- **Engineering, capacity, and load balancing** If you have a large number of Symposium Web Client or Agent Desktop Displays users in your environment, the engineering calculations may indicate performance limitations or very high application server specifications. In this case, you may be able to overcome these limitations by sharing the load across multiple application servers, with different users accessing different application servers in the network. For more information, see the *Symposium Call Center Server Planning and Engineering Guide*.

- **Redundancy** In mission-critical or 24-hour call centers, a multiple-application server configuration may provide redundancy or backup for the application servers.

Multiple servers in Symposium Call Center Server (Symposium Call Center Server network or independent sites)

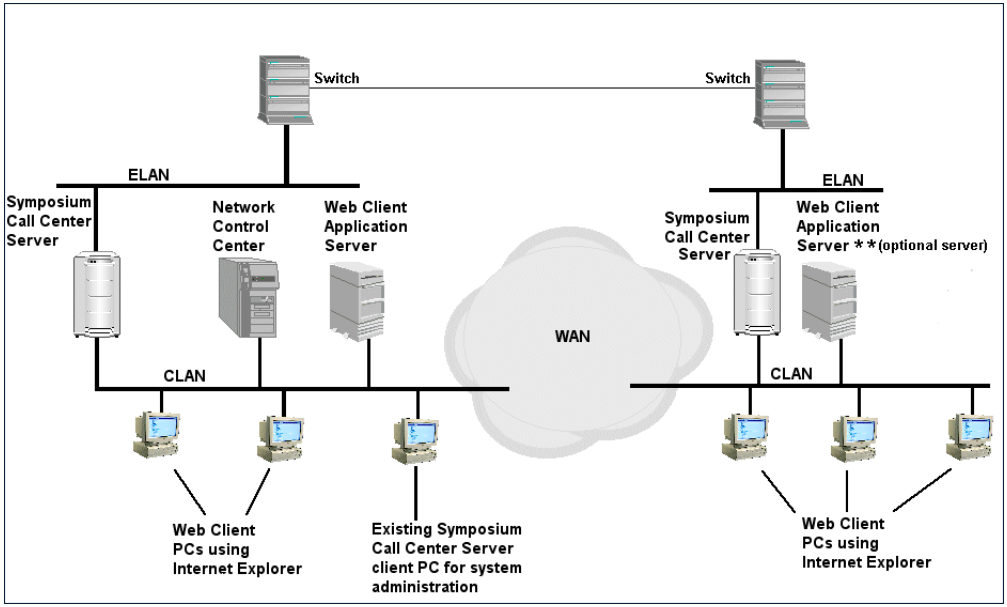
Each application server can be configured to manage multiple servers in Symposium Call Center Server simultaneously. This capability provides you with a unified view of multiple sites or locations, enabling you to manage multiple call centers with a single management tool—Symposium Web Client.

One Symposium Web Client application server can be paired with each server in Symposium Call Center Server, or one Symposium Web Client application server can be used across the entire network of servers in Symposium Call Center Server.

If you have multiple servers in your Symposium Call Center Server network, you may want to consider implementing a second Symposium Web Client application server for better response times. Multiple application servers can share the same user data (user preferences) by using Active Directory replication. For details on replication, and the limitations on data sharing, see “Symposium Web Client and replication” on page 65.

The following diagram depicts this type of configuration:

Multiple servers in Symposium Call Center Server



Considerations and decision criteria

Note the following when deciding whether to configure Symposium Web Client in a multiple node environment.

- **Engineering, capacity, and load balancing** If you have a large number of Symposium Web Client or Agent Desktop Displays users in your environment, the engineering calculations may indicate performance limitations or very high application server specifications. In this case, you may be able to overcome these limitations by sharing the load across multiple application servers, with different users accessing different application servers in the network. For more information, see the *Symposium Call Center Server Planning and Engineering Guide*.
- **Redundancy** In mission-critical or 24-hour call centers, a multiple-application server configuration may provide redundancy or backup for the application servers. Physical proximity of an application server at each of the sites may also help WAN fault tolerance.

- **Network traffic / network latency** A distributed multiple application server configuration may help reduce WAN traffic and provide faster response times to Symposium Web Client users at other sites. For more information, see the section on network engineering guidelines in the *Symposium Call Center Server Planning and Engineering Guide*.

Switches supported by Symposium Web Client

Symposium Web Client supports any switches that are supported by Symposium Call Center Server. These switches vary based on the version of Symposium Call Center Server. For details on the compatibility of Symposium Web Client and different versions of Symposium Call Center Server, see "Symposium Call Center Server requirements" on page 32. For details on the switches supported by Symposium Call Center Server, see the *Symposium Call Center Server Symposium, M1/CSE 1000, and Voice Processing Guide*.

User types in Symposium Web Client

It is important to understand the difference between the Symposium Web Client user and the Symposium Call Center Server user. You create each user in different Symposium Web Client components.

User type	User definition	Created in
Symposium Call Center Server user	agents, supervisors, supervisor/agents	Contact Center Management or Configuration
Web Client user	anyone who logs on to the application server and monitors the performance and activities of Symposium Call Center Server	Access and Partition Management
Windows 2000 user	administrators	Windows 2000

Skills you need

Installation and configuration knowledge

You must have knowledge of the following tasks to install Symposium Web Client:

- Microsoft Windows 2000 Advanced Server or Windows 2000 Server with Service Pack 3 (minimum), Service Pack 4 or later (recommended) installation, configuration, and maintenance

Note: As Service Packs for Windows 2000 become available, Nortel Networks tests them for compatibility against the Symposium Web Client software as soon as possible. Nortel Networks recommends that customers upgrade to new service packs as per vendor (Microsoft) recommendations, because critical service packs may include security enhancements.

- Microsoft Active Directory installation, configuration, and maintenance
- Microsoft Internet Explorer 5.5 with Service Pack 2 (minimum) or Internet Explorer 6.0 with Service Pack 1 or later (recommended) installation and configuration

Timing

The operating system installation and Symposium Web Client installation take approximately 3 hours to complete. This does not include the time that is required for pre-installation planning, switch configuration, or post-installation setup and configuration, such as adding agents.

Installation worksheets and checklists

For tips on installing Symposium Web Client and the operating system software, see Appendix A, “Installation worksheets and checklists.”

Related documents

Introduction

This section lists the documents in which you can find additional information about Symposium Web Client and Symposium Call Center Server.

If you need information about	Refer to
■ Real-Time Reporting, Historical Reporting, Contact Center Management, and Emergency Help	*Symposium Call Center Web Client Supervisor's Reference Guide*
■ the M1 Data Extraction Tool	*Symposium Call Center Web Client Data Extraction Tool User's Guide for the Meridian 1*
■ detailed historical reports	*Symposium Call Center Server Historical Reporting and Data Dictionary*
■ scripting	*Symposium Call Center Server Scripting Guide*
■ administering the Network Control Center	*Symposium Call Center Server Network Control Center Administrator's Guide*
■ switches	*Nortel Networks Symposium, M1/ CSE 1000, and Voice Processing Guide* or the *Nortel Networks Symposium Call Center Server Planning and Engineering Guide*

Note: If you are using the Symposium Configuration Tool only, then refer to Chapter 3, "Installing and configuring application server software," and Chapter 6, "Using Symposium Web Client," for information about the Configuration component.

System requirements

Introduction

Symposium Web Client can reside on any server on which Windows 2000 Server with Service Pack 3 (minimum), Service Pack 4 or later (recommended), or Windows 2000 Advanced Server is installed. From this point on, this document refers to this server as the application server. To access Symposium Web Client on the application server, the client PC must have Microsoft Internet Explorer 5.5 with Service Pack 2 (minimum) or Internet Explorer 6.0 with Service Pack 1 or later (recommended) installed.

Note: All system requirements and installation procedures apply to Symposium Web Client and the Symposium Configuration Tool.

Application server hardware requirements

Symposium Web Client runs on a dedicated computer on which Microsoft Windows 2000 Server with Service Pack 3 (minimum), Service Pack 4 or later (recommended), or Windows 2000 Advanced Server is installed. Nortel Networks does not supply this server; it can be customer- or distributor-supplied. Specific hardware requirements depend on your call center size. For expected performance measurements and related system requirements, see “Application server performance requirements” on page 32.

Symposium Web Client follows Microsoft’s “Designed for Windows 2000 Application Specification” standard. Since Symposium Web Client is a mission-critical application, Nortel Networks does not recommend sharing the Symposium Web Client application server with other “application” class software applications, which generally require a certain amount of system resources.

Note that running additional software (for example, virus scan software) may place an additional load on the Symposium Web Client application server. Therefore, you should set all utility tools to run on the application server during off-peak hours. In addition, all utilities installed on the application server must be included in Microsoft's Compatibility List for Windows 2000 Server. You can view this list at http://www.microsoft.com/windows2000/server/howtobuy/upgrading/compat/default.asp.

Notes:

- Nortel Networks does not provide support on the configuration of anti-virus software. Direct all your questions or problems on anti-virus software to the appropriate vendor.
- The above recommendations are intended as guidelines only, and do not constitute a guarantee of compatibility.
- If you raise performance or functionality issues to Nortel Networks support personnel, as part of the fault diagnosis process, the support technician may ask you to remove all third-party software from the application server.

Application server software requirements

- Windows 2000 Advanced Server or Windows 2000 Server Service Pack 3 (minimum) or Service Pack 4 or later (recommended) with Internet Information Services (IIS), Simple Mail Transfer Protocol (SMTP), Terminal Services, and Terminal Services Licensing (you require Terminal Services for the Script Editor portion of the Scripting component)

Notes:

- As Service Packs for Windows 2000 become available, Nortel Networks tests them for compatibility against the Symposium Web Client software as soon as possible. Nortel Networks recommends that customers upgrade to new service packs as per vendor (Microsoft) recommendations, because critical service packs may include security enhancements.
- Terminal Services can communicate with the Terminal Services License Server (Terminal Services Licensing) only if they are in the same domain. Therefore, Nortel Networks recommends that you install both on the application server because it is a domain controller.

- Windows Installer 2.0 or later (version 2.0 is included on the Symposium Web Client CD-ROM, and in Windows 2000 Server Service Pack 3)
- For more information about Windows 2000 requirements, see the "Windows 2000 Server/Advanced Server installation checklist" on page 550.

ATTENTION

As of the date of publication, the following information on Client Access Licensing was available from Microsoft. Consult Microsoft for the latest information. Nortel Networks does not accept any liability for end-user compliance with Microsoft licensing agreements. This information has been provided for your convenience.

- You must purchase from Microsoft both a Terminal Services Client Access License and a Windows 2000 Server Client Access License for each client PC running on Windows 98 or NT that will be accessing the Script Manager portion of the Scripting component.
- Client PCs running on Windows 2000 or Windows XP require a Windows 2000 Server Client Access License only; they do not require a separate Terminal Services Client Access License.
- Nortel Networks does not provide these Client Access Licenses.
- The Windows 2000 Server Client Access Licenses do not float (that is, they are specific to the client PCs for which they have been purchased).
- If the client PC is accessing only Script Variables or Application Thresholds, then these licenses are not required.

- Microsoft Active Directory
- Sybase Open Client v.12.5 (required for the Historical Reporting and Contact Center Management components; supplied by Nortel Networks)
- Microsoft Internet Explorer 5.5 with Service Pack 2 (minimum) or Internet Explorer 6.0 with Service Pack 1 or later (recommended). This is required

so support personnel can access the application server. For information on upgrading from Internet Explorer version 5.0, see “Upgrading Internet Explorer on the application server” on page 113.

Notes:

- As Service Packs for Internet Explorer become available, Nortel Networks tests them for compatibility against the Symposium Web Client software as soon as possible. Nortel Networks recommends that customers upgrade to new service packs as per vendor (Microsoft) recommendations, because critical service packs may include security enhancements.
- To install, uninstall, and configure Symposium Web Client, you must have administrator privileges on the application server.

Client hardware requirements

Note: The following client requirements also apply to PCs running Agent Desktop Displays:

- Pentium II 300 or better
- 20 Mbytes of available hard disk space for the Agent Desktop Displays component
- a minimum of 64 Mbytes of RAM
- a minimum 800 x 600 pixel resolution monitor (1024 x 768 pixel resolution is recommended for optimal display quality)
- a serial port (if connection of the M1 Data Extraction Tool to the M1 switch using a serial port is required)

Note: If you are going to connect to the M1 switch, you can use either the client PC or the application server as long as the system you use has a serial port. The M1 Data Extraction Tool is intended for use with the M1 switch only; it may not support the Meridian 1 Internet Enabled switch.

The Pentium II 300 MHz configuration should be adequate for normal operation in small call centers (less than 50 agents). For more intensive activity and larger call centers, a faster processor and additional RAM, or both, improves performance. For larger call centers and higher levels of activity, the minimum platform should be scaled up accordingly.

Client software requirements

Note: The following client requirements also apply to PCs running Agent Desktop Displays:

- Windows 98 Second Edition, Windows NT 4.0 Workstation Service Pack 6a, Windows 2000 Professional, Windows 2000 Server, Windows 2000 Advanced Server, or Windows XP Professional
- Windows Installer 2.0 or later. Version 2.0 is included on the Symposium Web Client CD-ROM, and in both Windows 2000 Service Pack 3 for Windows 2000 Server and Professional, and Windows XP. If the client PC runs any other operating system, then you must install the software from the Symposium Web Client CD-ROM.
- Microsoft Internet Explorer 5.5 with Service Pack 2 (minimum) or Internet Explorer 6.0 with Service Pack 1 or later (recommended)

Note: As Service Packs for Internet Explorer become available, Nortel Networks tests them for compatibility against the Symposium Web Client software as soon as possible. Nortel Networks recommends that customers upgrade to new service packs as per vendor (Microsoft) recommendations, because critical service packs may include security enhancements.

- Excel 2000 Service Release 1a (required for the Configuration component only)
- Microsoft Data Access Components (MDAC) v.2.5 or later (required for Windows 98 and NT 4.0 Workstation; version 2.5 is included on the Symposium Web Client installation CD)
- Simple Object Access Protocol (SOAP) version 3.0 merge module (a Microsoft standard component required by all clients running Windows 98, NT 4.0 Workstation, XP, Windows 2000 Professional, Windows 2000 Server, or Windows 2000 Advanced Server; the installation file, ClientSoap.msi is included in the root directory of the Symposium Web Client installation CD)

Note: Supervisors who connect to Symposium Web Client on a client PC running Windows 2000 must have administrator rights on the client PC to receive the required Active X downloads that enable their Internet Explorer browser to work correctly.

Client backward compatibility

When you use the client PC to connect to an application server running Symposium Web Client 4.5, the system automatically downloads the required third-party controls onto the client PC. However, you can still use this same client PC to connect to an application server running Symposium Web Client 4.0, in addition to the server running Symposium Web Client 4.5.

The exception to this rule occurs when you download and install the Agent Desktop Displays 4.5 client software onto the client PC. In this case, you cannot use the Agent Desktop Displays 4.5 component when connected to an application server running Symposium Web Client 4.0. Nortel Networks recommends, therefore, that while working in an environment with both releases of the Symposium Web Client software, do not upgrade the Agent Desktop Displays client software to Release 4.5. For more information, see “Versions of Agent Desktop Displays and compatibility with Symposium Web Client” on page 321.

Note: You can use the Agent Desktop Displays 4.0 client to connect to both Symposium Web Client 4.0 and 4.5 application servers. However, in this case, the communication between the client PC and application server continues to be through Remote Data Service (RDS), rather than SOAP, which is new to Release 4.5. Therefore, the RDS communication method must be enabled on the application server for Agent Desktop Displays 4.0 to function properly.

The RDS communication method is installed and enabled by default on the application server. However, if you have performed the IIS Lockdown procedure and you have removed the MSADC virtual directory, then you have disabled RDS. If you want to reenable RDS on the application server, then you must recreate the MSADC virtual directory in IIS. For more information, see “To reenable Remote Data Service” on page 244.

Client coresidency

In Symposium Web Client, the client PC contains the following components:

- Internet Explorer 5.5 (or later)
- Simple Object Access Protocol (SOAP) version 3.0 merge module (a Microsoft standard component)
- Agent Desktop Displays client application

- Symposium Configuration Tool spreadsheets
- M1 Data Extraction Tool

These components are capable of coresiding with the following products:

- Symposium Call Center Server 4.0 Client
- Call Pilot Web Administration Client 2.0
- Optivity Telephone Manager (OTM) 2.0
- i2050 Software Phone
- Symposium Web Center Portal Agent Client 4.0
- Symposium Web Center Portal Administration/Supervisor Client 4.0
- Symposium Express Call Center Client 4.0
- Microsoft Office 2000 and XP

Symposium Call Center Server requirements

- Symposium Web Client is compatible with either Symposium Call Center Server Release 4.0 (NS040107SU10S) or later, or Symposium Call Center Server Release 4.2 (NS040206SU08S) or later. Symposium Web Client is incompatible with previous releases of Symposium Call Center Server.

Application server performance requirements

The call center parameters that are shown in the following table (for example, the total number of active agents) can reside on one server in Symposium Call Center Server, or they can reside across multiple servers in a networked call center. For example, if you have a Pentium IV 1.4 GHz or equivalent, then the recommended load is 1000 agents.

In a single node environment, the 1000 agents reside on the single server. In a network consisting of three call center servers, approximately 333 agents (or a similar variation so that the total number of active agents does not exceed 1000) can reside on each server. If any of the parameters exceed the load that is specified in the tables, then Nortel Networks recommends that you use a higher

performance platform as the application server, or use more than one application server. For details on application server sizing requirements, see “Application server sizing requirements” on page 35. For more information, see the *Symposium Call Center Server Planning and Engineering Guide*.

Recommendations	for this load
■ Pentium III 733 or better ■ 512 Mbytes of RAM ■ 20 Gbytes of disk space ■ NIC	**Call Center Parameters:** ■ up to 250 active agents ■ 50 skillsets ■ 50 applications ■ 20 IVR queues ■ 128 routes **per Symposium Web Client application server:** ■ 25 Symposium Web Client users (excluding Agent Desktop Display users) ■ 250 Agent Desktop Display users
■ Pentium IV 1.4 GHz * ■ 1.0 Gbyte of RAM ■ 40 Gbytes of disk space ■ NIC	**Call Center Parameters:** ■ 1500 active agents ■ 350 skillsets ■ 500 applications ■ 50 IVR queues ■ 250 routes

Recommendations	for this load
	per Symposium Web Client application server: ■ 150 Symposium Web Client users (excluding Agent Desktop Display users) ■ 1000 Agent Desktop Display users

* Pentium IV 1.4 GHz or equivalent (for example, a dual Pentium III with equivalent CPU processing power)

Note: The minimum hard disk space requirements are recommended for the Symposium Web Client application software, Crystal Reports templates, historical reports, log files, and exported real-time displays.

Although an Intel Pentium III 733 MHz processor with 512 Mbytes of RAM meets the basic hardware requirements for running Symposium Web Client with the smaller call center configurations, a faster processor and additional RAM, or both, will improve the performance of the system for most operations.

The generation of large call-by-call reports can create temporary files of 1 Gbyte or more and can be time consuming. A faster system is highly preferred if the end user is managing a large number of objects (greater than 1000), such as call center agents, or generating large historical or call-by-call reports, or both.

Additional parameters

Refresh rates: The minimum refresh rate on the application server is .5 seconds. You can adjust this rate to achieve optimal balance between latency and CPU consumption.

Historical reports: The combined number of ad hoc or scheduled reports that you can generate simultaneously is limited to five. You can schedule as many historical reports as required; however, only five scheduled reports are processed simultaneously while the others wait in queue. Likewise, for ad hoc reports, only five reports can be generated at the same time. For example, five supervisors can generate an ad hoc report, but the sixth supervisor to do so receives a message saying the system could not process the request. This supervisor must try to

generate the ad hoc report again later, after the first five reports have been generated (or schedule the report to run later). This limitation applies to the *total* of the ad hoc and scheduled reports that can be generated at a particular time. For example, if two reports are scheduled to be output at noon, then only three ad hoc reports can be generated at this time, bringing the total to five.

Application server sizing requirements

The table below provides recommendations for sizing requirements of the application server based on the following typical call center usage patterns:

- The ratio of agents to supervisors does not exceed 10 (10 agents per supervisor).
- Average CPU utilization does not exceed 70 percent over at least a 15-minute period during peak usage loads (see “CPU utilization on the application server and client PC” below).
- The number of requests from each user to the application server does not exceed 17 per minute.

CPU utilization on the application server and client PC

The application server employs an Intel Pentium processor. The minimum recommended processor is the Pentium III with a clock speed of 733 MHz, 512 Mbytes of memory, and a 20 Gbyte hard drive.

For optimal performance, the average CPU utilization on both the application server and the client should not exceed 70 percent over at least a 15-minute time period. However, it is expected and quite normal for the CPU utilization to exceed the 70 percent limit (up to 100 percent) for relatively short periods of time.

Note: To help you estimate the CPU impact on the Symposium Web Client Application Server and to estimate the CPU impact from the real-time displays on the client PC, you can use the Web Client CPU utilization analysis spreadsheet. This spreadsheet is available on the Channel Readiness portion of the Partner Information Center (PIC) web site at www.my.nortelnetworks.com, within the Symposium Web Client section (you require level 4 access to download this file).

You can perform the following measures to reduce CPU load:

Application Server

- Reduce RTD refresh rates.
- Stagger scheduled historical reports so that they are not scheduled to run at the same time.
- Schedule large reports to run at off-peak hours.
- Schedule antivirus scanning to occur at off-peak hours.
- Perform backup/restore procedures at off-peak hours.

Client PC

- Reduce RTD refresh rates.
- Configure the client to display less data by using data partitioning.

Note: The following table outlines some sample figures of the processor speed required to support some different call center sizes and configurations.

Maximum number of supported agents across the network	Maximum number of supported Web Client users (excluding ADD users)	Processor
466	47	PIII 733 MHz
472	47	PIII 750 MHz
502	50	PIII 800 MHz
542	54	PIII 866 MHz
586	59	PIII 933 MHz
620	62	PIII 1.0 GHz
785	78	PIV 1.3 GHz
917	92	PIV 1.5 GHz
715	72	Dual PIII 733 MHz

Maximum number of supported agents across the network	Maximum number of supported Web Client users (excluding ADD users)	Processor
725	72	Dual PIII 750 MHz
769	77	Dual PIII 800 MHz
830	83	Dual PIII 866 MHz
895	89	Dual PIII 933 MHz
946	95	Dual PIII 1.0 GHz
1193	119	Dual Xeon 1.4 GHz
1391	139	Dual Xeon 1.5 GHz

Note: If the parameters are exceeded, then you can use more than one application server, and you can split Web Client users across the multiple application servers.

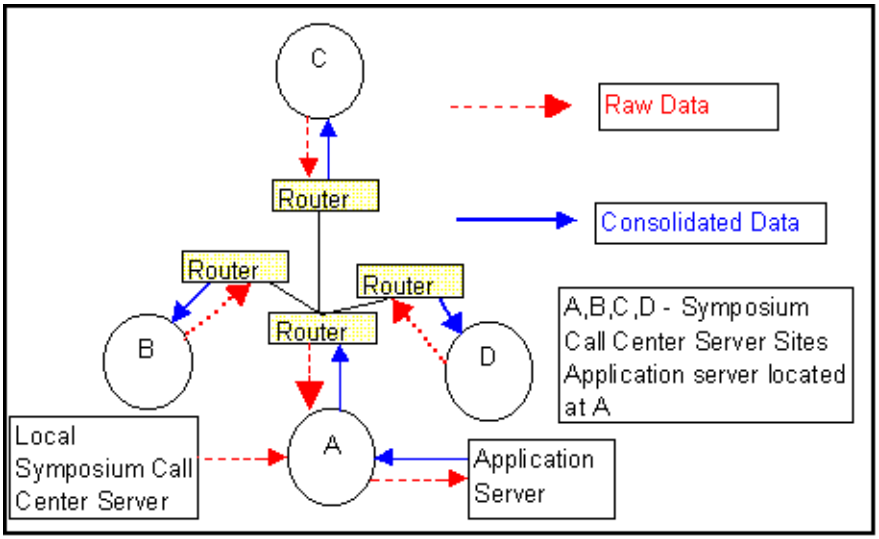
Multicast LAN/WAN impact

The multicast LAN/WAN impact from the application server can be broken down into two parts:

- nodal real-time display multicast data
- network-consolidated real-time display (NCRTD) data

The server in Symposium Call Center Server sends nodal real-time display multicast data to the application server. The impact of this data is described in the *Symposium Call Center Server Planning and Engineering Guide*.

The application server consolidates the multicast traffic from one or more servers in Symposium Call Center Server into a single, network consolidated, multicast stream. This stream is sent from the application server to the client PCs anywhere in the network.



In the above diagram, there is one application server located at node A. All the servers in Symposium Call Center Server send raw real-time data to the application server. The application server, in turn, sends consolidated data out to all of the Symposium Web Client client PCs.

The consolidated real-time traffic that the application server sends to clients requesting this data is approximately equal to the sum of all the raw data. There is very little compression performed.

Note: The total LAN/WAN impact due to multicast NCRTD traffic can be estimated using the Symposium Call Center Server Capacity Assessment Tool. For more information on this tool and on the LAN/WAN impact, see the *Symposium Call Center Server Planning and Engineering Guide*.

You can also use the Web Client CPU utilization analysis spreadsheet to estimate the CPU impact on the Symposium Web Client Application Server and to estimate the CPU impact from the real-time displays on the client PC. This spreadsheet is available on the Channel Readiness portion of the Partner Information Center (PIC) web site at www.my.nortelnetworks.com, within the Symposium Web Client section (you require level 4 access to download this file).

Unicast LAN/WAN impact

In addition to the multicast data that the application server sends to the client PCs, it sends unicast real-time data over the CLAN to the client PCs that cannot receive multicast data. The calculations used to determine the LAN utilization due to this unicast traffic are almost identical to those used to calculate the impact of the multicast traffic, as described in the previous section.

Note: This traffic may also be sent over the WAN in response to remote client requests.

The presence of these unicast clients in a Symposium Web Client configuration results in additional network traffic. Unicast clients use dedicated point-to-point connections, so each client receives its own data stream.

Whereas the application server sends only one multicast stream to each site requesting multicast real-time data, it sends multiple streams of unicast real-time data according to the following rules:

For a given client PC, the server sends no more than one stream to support at least one display of the same data type. There are 12 data streams in total, 6 streams for each type of data that is viewed in either of the two data collection modes (interval to date or moving window), as follows:

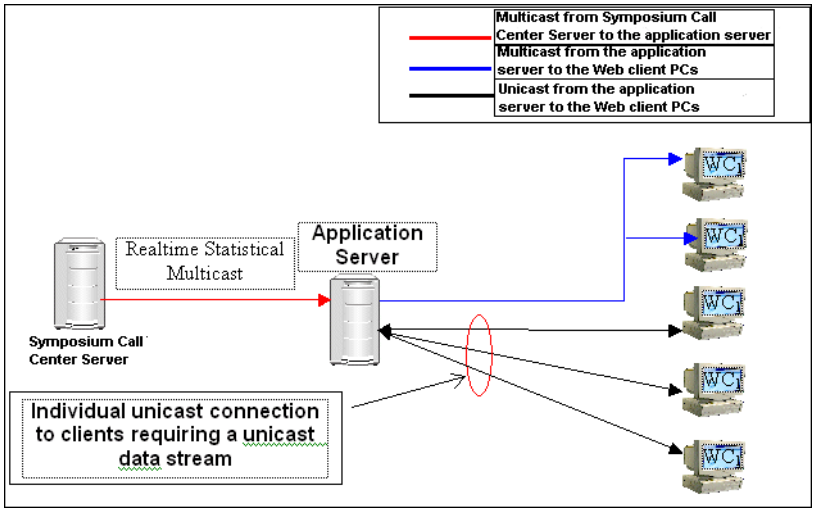
- 6 streams of **interval to date** data (agent, skillset, application, nodal, IVR, and route)
- 6 streams of **moving window** data (agent, skillset, application, nodal, IVR, and route)

For example, if the same client opens two Agent/moving window displays, then the server sends only one Agent/moving window data stream.

Note: The size of each data stream is identical to the corresponding multicast stream.

The diagram on the page below shows the single, shared multicast stream, which can provide data to any number of clients, and the dedicated unicast streams to each of the unicast clients.

To help you estimate the network traffic impact on both the CLAN and WAN when deploying the Symposium Web Client Application Server, you can use the Web Client multicast and unicast traffic analysis spreadsheet. This spreadsheet is available on the Channel Readiness portion of the Partner Information Center (PIC) web site at www.my.nortelnetworks.com, within the Symposium Web Client section (you require level 4 access to download this file).



Disk partitions and communication ports

Introduction

This section provides high-level information on disk partitions. It also provides TCP/UDP port numbers that are used by Symposium Web Client.

Protecting your data

To protect your data, you can take the following precautions:

- Install the operating system and Symposium Web Client on an NT File System (NTFS) partition. File Allocation Table (FAT) partitions do not support security.

Note: Since there are no specific guidelines or restrictions regarding the number or size of the application server disk partitions for Symposium Web Client, the person installing the software must determine the best hard disk configuration for the application server. For example, there can be separate disk partitions for the operating system, the application software, and the shared folders that are required for exporting historical reports, or everything can be installed and configured on the same disk partition.

Refer to the “Windows 2000 Server/Advanced Server installation checklist” on page 550 for information about installing Windows 2000.

Communication ports

The following table lists the TCP/UDP ports that Symposium Web Client uses with the application server. You can use this information for items such as firewall implementation, or identifying potential port conflicts within the client PC or the application server. To minimize the potential points of failure (in a nodal call center setting), place the server in Symposium Call Center Server and the Symposium Web Client application server on the same subnet.

Port number	Functionality	Port location
■ Port 80	for Internet Explorer's communication	application server
■ Port 3389	for Terminal Services' communication	application server
■ Port 25 (SMTP)	for the Historical Reporting component to send e-mail notifications when reports are printed and saved	application server
■ Port 8200	for the Emergency Help component	client PC
■ UDP ports 6020, 6030, 6040, 6050, 6060, 6070, 6080, 6090, 6100, 6110, 6120, 6130	for the application server to receive IP multicasting data from Symposium Call Center Server (needed for Real-Time Reporting and Agent Desktop Displays)	application server
■ UDP ports 7020, 7030, 7040, 7050, 7060, 7070, 7080, 7090, 7100, 7110, 7120, 7130	for the application server to send IP multicasting data to client PCs (needed for Real-Time Reporting and Agent Desktop Displays)	client PC

Port number	Functionality	Port location
■ UDP ports 7025. 7035, 7045, 7055, 7065, 7075, 7085, 7095, 7105, 7115, 7125, 7135	for the application server to send IP unicast data to client PCs. This is an optional method of sending the data required for Real-Time Reporting. If you do not use the multicast method, then you must configure the unicast option. You can also use a combination of the two methods.	client PC

Note: Based on your network configuration and the amount of access to the application server that is required (for example, for print servers and file sharing), you may also need to configure domain trust relationships and firewalls. For more information on this additional configuration, consult the Microsoft guidelines on Windows 2000 networking.

Symposium Web Client and Crystal Reports

Introduction

The Symposium Web Client installation includes some Crystal Reports 9.0 components that enable you to run and view the standard historical reports in the Symposium Web Client Historical Reporting component; the installation does not include report writing software. To create your own custom reports for use with Symposium Web Client, you must purchase and install Crystal Reports 9.0.

Crystal Reports versions supported

To create custom reports that are compatible with Symposium Web Client, you must purchase and install the Professional or Developer version of Crystal Reports 9.0, which is available only as an upgrade from Crystal Reports versions 8.0 or 8.5. The Standard version of Crystal Reports is not supported.

Crystal Reports and the application server

For performance purposes, and to avoid coresidency problems. it is best to install Crystal Reports on a PC other than the application server. However, if you must install Crystal Reports on the application server, see the following sections.

Installation tips for Crystal Reports 9.0

Crystal Reports 9.0 is available only as an upgrade from version 8.0 or 8.5. Therefore, regardless of where you install Crystal Reports 9.0 (either on the application server, or another server of your choice), the server must contain an installation of Crystal Reports version 8.0 or 8.5 before you install version 9.0.

- **Installation order** You can install Crystal Reports 9.0 on the application server either before or after you install Symposium Web Client. However, the application server must contain either Crystal Reports 8.0 or 8.5 before you install Crystal Reports 9.0.
- **Uninstalling Symposium Web Client** After you install Crystal Reports 9.0 and Symposium Web Client on the application server, should you need to uninstall Symposium Web Client, then your Crystal Reports installation is corrupted because some of its components are also removed. In this case,

to continue to use Crystal Reports, you must repair or reinstall Crystal Reports 9.0.

- **Uninstalling Crystal Reports 9.0** After you install Crystal Reports 9.0 and Symposium Web Client on the application server, should you need to uninstall Crystal Reports, it impacts the Historical Reporting component. In this case, you can repair the Historical Reporting component by installing the Crystal Reports 9.0 merge modules from the Symposium Web Client CD-ROM. To do this, in the root directory of the CD, locate and double-click the file CRTemplates.msi. A Windows Installer package automatically installs the modules.

Chapter 2

Preparing Symposium Call Center Server

In this chapter

Overview 48

Modifying Real-time Statistics Multicast settings 49

Testing the Real-time Statistics Multicast service 58

Overview

Introduction

The Symposium Web Client application server uses the Real-time Statistics Multicast (RSM) service to send real-time data from Symposium Call Center Server to Symposium Web Client users. The two Web Client components that require this functionality are Real-Time Reporting and Agent Desktop Displays.

Before Symposium Web Client can send and receive multicast data, RSM must be installed and configured on the server in Symposium Call Center Server.

The RSM service is installed during the Symposium Call Center Server installation. During installation, the system verifies that you have the correct RSM keycode, and then installs the required RSM files on the server.

When you install RSM, you must provide the IP multicasting address that the server in Symposium Call Center Server uses to transmit RSM data to the Web Client application server. The system automatically sets the default port numbers and multicast rates for real-time statistics during installation.

For more detailed information on installing the RSM feature in Symposium Call Center Server, see “Installing the Server Software” or “Converting, upgrading, reinstalling, and uninstalling server software” in the *Symposium Call Center Server Installation and Maintenance Guide*.

This chapter explains how to perform the following procedures in Symposium Call Center Server:

- Modify the default RSM settings and multicast rates. See “Modifying Real-time Statistics Multicast settings,” on page 49 for more information. You must modify the default RSM settings; otherwise, no data is sent from the server in Symposium Call Center Server to the Symposium Web Client application server.
- Verify that the RSM service is sending data to the appropriate ports. See “Testing the Real-time Statistics Multicast service,” on page 58 for more information.

Modifying Real-time Statistics Multicast settings

Introduction

You can modify RSM's default settings on each server in Symposium Call Center Server to reflect the requirements of your organization:

- You can activate or deactivate the collection of up to six types of real-time statistics using the RTD Multicast Controller Utility (MulticastCtrl.exe).
- You can modify the following multicast settings using the RTD Multicast Configuration Utility (RSMConfg.exe):
  - the IP multicast address
  - the Time To Live (TTL) value for the IP multicast data
  - the IP ports that send the real-time statistics
  - the multicast rates for the IP ports that send the real-time statistics

Activating or deactivating the collection of real-time statistics

You can select which statistics the RSM service collects and how they are collected using the RTD Multicast Controller utility.

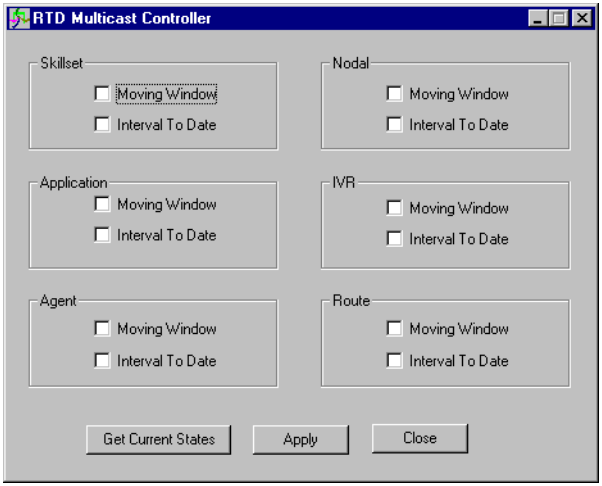
To activate or deactivate the collection of real-time statistics

1 Navigate to the folder in which the RSM component is installed:

[drive]:\Nortel\iccm\bin

2 Double-click **MulticastCtrl.exe**.

Result: The RTD Multicast Controller window appears.



3 Click the **Moving Window** or **Interval To Date** check boxes, or both, for each real-time statistics group that you want to collect.

Note: Nortel Networks recommends that you click Moving Window and Interval To Date for all statistics groups, so both options are available for all statistics in Symposium Web Client.

The Meridian 1 and Succession Communication Server for Enterprise 1000 switch (M1/CSE 1000) real-time statistics groups are

- Skillset
- Application
- Agent
- Nodal
- Route
- IVR

The Digital Multiplex Switch/Meridian Stored Logic-100 switch (DMS/MSL-100) real-time statistics groups are

- Skillset
- Application

- Agent
- Nodal

4 Click **Apply**.

5 Click **OK** to close the window.

Modifying RSM settings and multicast rates

Perform the following steps to modify RSM settings and multicast rates in Symposium Call Center Server.

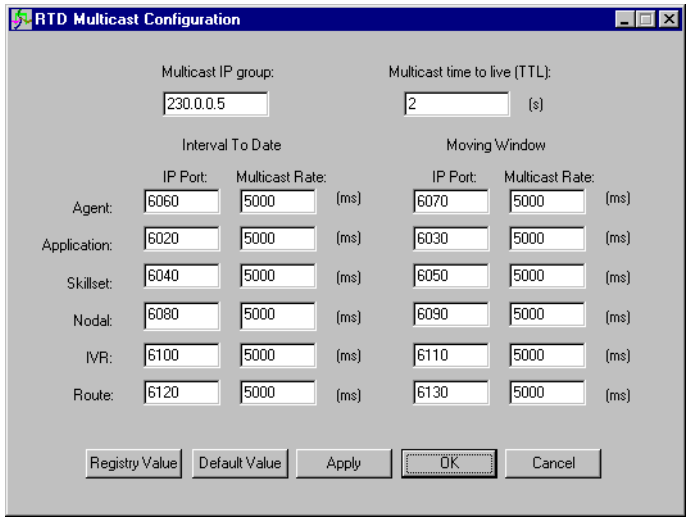
To modify RSM settings and multicast rates

1 Navigate to the folder in which the RSM component is installed:

[drive]:\Nortel\iccm\bin

2 Double-click **RSMConfg.exe**.

Result: The RTD Multicast Configuration window appears.



ATTENTION

The IP multicast addresses that support multicasting are 224.0.0.0 through 239.255.255.255, *but* the IP multicast addresses between 224.0.0.0 and 224.0.0.255 inclusive are reserved for routing and topology discovery or maintenance protocols, and should not be used.

Check the Internet Engineering Task Force (http://www.ietf.org) and Internet Assigned Numbers Authority (http://www.iana.org) web sites to review a complete list of reserved IP multicast addresses before you select an address for your internal multicast needs.

For more information about IP Multicasting, see "Implementing IP multicasting for Symposium Web Client" on page 571.

3 In the **IP Multicast group** box, type the IP multicast address that has been designated as the sending address for IP multicasting in Symposium Call Center Server.

4 Accept the default IP port numbers for each statistics group.

ATTENTION

Do not change the default IP port numbers assigned to the statistics groups. Symposium Web Client's Real-Time Reporting component receives multicast statistics through these ports and will malfunction if the port numbers are changed.

5 Change the Multicast time to live (TTL) value to a value that is appropriate for your network.

ATTENTION

If packets are traveling through more than one router, you should change the Multicast TTL value to a value that is appropriate for your network and the number of routers that you use. If the TTL value is set too low, the real-time multicast statistics may not reach your application. The Default TTL value is 2 hops. Nortel Networks recommends a value between 64 and 68 hops.

6 Accept the default multicast rates (5 seconds) in the **Multicast Rate** boxes.

ATTENTION

The fastest rate at which multicast data from Symposium Call Center Server can reach the end user in Symposium Web Client is equal to the highest value among the following settings:

- the Multicast Rate at which data is sent from Symposium Call Center Server to the Symposium Web Client application server
- the Output Rate at which the application server outputs data to client PCs
- the Transform Rate at which the application server processes real-time statistics

The delay between the data being sent from the server in Symposium Call Center Server and arriving at the client PC is a function of all these rates; the rates on the server in Symposium Call Center Server and the application server are not synchronized. If you want to decrease the length of time required for real-time statistics to reach client PCs, you can decrease the Output Rate and Transform Rate values; however, this impacts performance on the application server. You should notify users of the Real-Time Reporting component of these rates so they can adjust the refresh rate in Real-Time Reporting accordingly.

Example

If the Symposium Call Center Server Multicast Rate is set to 2 seconds, the application server Transform Rate is set to 1 second, and the application server Output Rate is 7 seconds, then the data on the client PC will not refresh faster than every 7 seconds, regardless of the refresh rate that the user has chosen in Real-Time Reporting.

You can adjust the default multicast rates in Symposium Call Center Server to a minimum value of 0.5 seconds; however, reducing the multicast rates increases the workload on Symposium Call Center Server. Adjust these rates only if you are certain that Symposium Call Center Server can handle the additional workload. For information on adjusting rates and assessing performance, see the Capacity Assessment Tool (CapTool) chapter of the *Symposium Call Center Server Planning and Engineering Guide*.

Tip: If you have made an error in modifying the multicast IP group, TTL, IP ports, or the multicast rates for each port, you can restore the original values by clicking **Registry Values** or **Default Values**. If you modify any of these values and click **OK** or **Apply**, the appropriate registries are updated with your changes. If you click **Registry Values** after the modifications have been saved to the registry, it has no effect.

- Click **Registry Values** before you click **Apply** to retrieve the values stored in the registries. Use this option if you want to cancel a change without having to remember and retype the original values.
- Click **Default Values** to restore the values that are set when Symposium Call Center Server is installed. Use this option if you have saved changes to the registry that have caused RSM-dependent applications to malfunction, and you want to begin again with the default RSM configuration.

7 Click **OK**.

ATTENTION

To activate new RSM settings on Symposium Call Center Server (with the exception of the multicast rates), you must stop and start the Statistical Data Propagator (SDP) service. For more information, see “To activate modifications to the RSM settings: multicast IP group, TTL, and IP port” on page 56.

To activate new multicast rate settings on Symposium Call Center Server, you must open the configuration utility and click **Apply**. Then, you must stop and restart the SDP service. For more information, see “To activate modifications to multicast rates” on page 55.

Activating modifications to multicast rates and RSM settings

When you modify multicast rates, RSM continues to transmit data at the original rate until you open the Multicast Controller utility and click **Apply**. Then, activate the change on Symposium Call Center Server by stopping and starting the Statistical Data Propagator (SDP) service.

You must also stop and start the SDP service when you modify the following RSM settings: the multicast IP group, TTL and IP port settings.

ATTENTION

When you stop the SDP service, Symposium Call Center Server stops sending RSM data to the Symposium Web Client application server, and real-time displays do not receive data during this time; therefore, Nortel Networks recommends that you stop and start the SDP service during non-peak hours.

To activate modifications to multicast rates

When you change a multicast rate in the RTD Multicast Configuration utility, you are only modifying the default value, not the current transmission rate. RSM continues to transmit data at the current rate until you open the RTD Multicast Controller utility and click **Apply**. After you click **Apply** in the RTD Multicast Controller utility, you must stop and restart the SDP Service.

1 Navigate to the folder in which the utility is installed:

[drive]:\Nortel\iccm\bin

2 Double-click **MulticastCtrl.exe**.

Result: The RTD Multicast Controller window appears.

3 Click **Apply**.

4 Click **Close**.

5 Click Start → Programs → Administrative Tools → Services.

Result: The Services window opens.

6 From the list of services, select the SDP_Service.

7 Click **Stop**.

8 Click **Start**.

Result: The system retrieves the new multicast rates from the appropriate registry, and RSM begins transmitting at the new rate.

9 Click **Close**.

Tip: If you are having problems stopping and starting the SDP_Service, you can temporarily disable it. When you disable the SDP_Service, it automatically stops running. After the service is disabled, reset it to start automatically, and then restart the service.

a. In the Services window, click the **SDP_Service**.

b. Click **Startup**.

Result: The Service dialog box appears.

c. Click **Disabled**.

Result: The SDP_Service is disabled.

d. Click **OK** to return to the Services window.

e. With the SDP_Service highlighted, click **Stop**.

Result: The SDP_Service stops.

f. Click **Startup**.

Result: The Service dialog box appears.

g. Click **Automatic**.

Result: The SDP_Service is set to automatically start when the system starts.

h. Click **OK** to return to the Services window.

i. With the SDP_Service highlighted, click **Start** to restart the service.

j. Click **Close**.

To activate modifications to the RSM settings: multicast IP group, TTL, and IP port

1 Click Start → Settings → Control Panel.

2 Click **Services**.

Result: The Services window opens.

3 From the list of services, select the SDP_Service.

4 Click **Stop**.

5 Click **Start**.

6 Click **Close**.

Tip: If you are having problems stopping and starting the SDP_Service, you can temporarily disable it. When you disable the SDP_Service, it automatically stops running. After the service is disabled, reset it to start automatically, and then restart the service.

a. In the Services window, click the SDP_Service.

b. Click **Startup**.

Result: The Service dialog box appears.

c. Click **Disabled**.

Result: The SDP_Service is disabled.

d. Click **OK** to return to the Services window.

e. With the SDP_Service highlighted, click **Stop**.

Result: The SDP_Service stops.

f. Click **Startup**.

Result: The Service dialog box appears.

g. Click **Automatic**.

Result: The SDP_Service is set to automatically start when the system starts.

h. Click **OK** to return to the Services window.

i. With the SDP_Service highlighted, click **Start** to restart the service.

j. Click **Close**.

Testing the Real-time Statistics Multicast service

Introduction

After you have installed RSM on Symposium Call Center Server, or modified RSM and restarted SDP_Service, you can test the RSM service by using the Multicast Receive utility (mRcv.exe). The Multicast Receive utility displays statistical information according to the settings specified in a configuration file called mRcv.ini.

Configuring the Multicast Receive utility

The Multicast Receive utility tests the RSM service's send capabilities one port at a time. You can specify which IP address and port the utility should monitor in the [MCast] section of the mRcv.ini file.

To modify the mRcv.ini file

1 Navigate to the folder in which the utility is installed:

[drive]:\Nortel\iccm\bin

2 Use a text editor to open mRcv.ini.

3 Modify the IP address or the port number, or both.

Note: The port numbers listed within the section bordered by # symbols in the .ini file are for reference only and list all of the acceptable port numbers that you can use in your test. See "Sample mRcv.ini file" on page 59 for an example of the information contained in a standard mRcv.ini file.

Example

If you want to test receipt of Skillset - Interval to date data, check the port number for Skillset - Interval to date in the .ini file, and then change the Port= setting in the [MCast] section to that port number. If Skillset - Interval to date = 6040 in the .ini file, the [MCast] section of the .ini file should be modified as follows:

[MCast]
IP=234.5.6.7
Port=6040

ATTENTION
The IP= value must match your IP multicast address.

4 Save the mRcv.ini file. After setting the parameters for your test, you can start mRcv.exe to begin the test. For more information, see “To start the mRcv application” on page 60.

Sample mRcv.ini file

The sample below is the default mRcv.ini file provided by the Symposium Call Center Server installation. When you run the mRcv.exe utility, it uses this .ini file to display Skillset - Moving window data sent by RSM based on the settings in the [MCast] section at the bottom of the file (IP = 234.5.6.7 Port = 6050).

Note: The list of port numbers in the mRcv.ini file is for reference only, and each line is “commented out” with the # symbol. You can use these port numbers as an easy-to-access list of valid ports that are being used in the system to display data. The only portion of the .ini file that can be modified is the [MCast] section at the bottom of the file.

##
#
 # mRcv.ini file
#
 # Valid port numbers are:
 # Application - Interval to date = 6020
 # Application - Moving window = 6030
 # Skillset - Interval to date = 6040
 # Skillset - Moving window = 6050
 # Agent - Interval to date = 6060
 # Agent - Moving window = 6070
 # Nodal - Interval to date = 6080
 # Nodal - Moving window = 6090
 # IVR - Interval to date = 6100
 # IVR - Moving window = 6110
 # Route - Interval to date = 6120
 # Route - Moving window = 6130

```
############################################################
[MCast]
IP = 234.5.6.7
Port = 6050
```

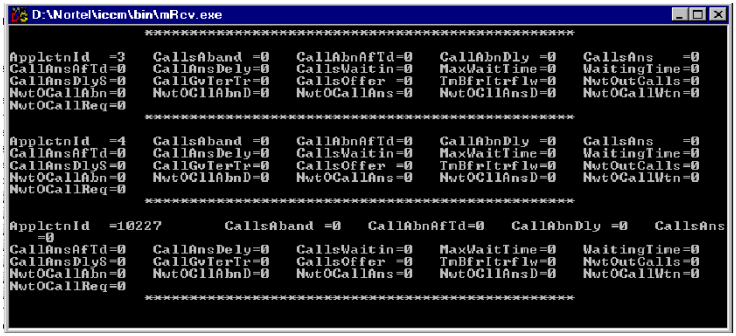
To start the mRcv application

1 Navigate to the folder in which the utility is installed:

[drive]:\Nortel\iccm\bin

2 Double-click **mRcv.exe**.

Result: The Multicast Receive utility opens in a console window, displaying data from the port and IP address that you specified in the mRcv.ini file.



Note: mRcv.exe displays *all* data received on the selected port, including data that is not recognizable by RSM. All non-RSM data is identified as “Not recognized by RSM.”

Chapter 3

Installing and configuring application server software

In this chapter

Overview 62

Section A: Windows 2000 server 63

Section B: Installing third-party software on the application server 73

Section C: Installing Symposium Web Client on the application server 95

Section D: Backing up and restoring user data 145

Section E: Configuring the application server 163

Section F: Security and the application server 197

Overview

Introduction

Before you install Symposium Web Client software or third-party software on your application server, be sure to complete the “Pre-installation worksheet” on page 537. Also, follow the “Installation checklist” on page 545 to ensure that you install and configure all software in the correct order.

If you are using the Real-Time Reporting component or the Agent Desktop Displays component, refer to Chapter 2, “Preparing Symposium Call Center Server” before you proceed with the instructions in this chapter.

This chapter explains how to complete the following procedures:

- installing and configuring Windows 2000 Advanced Server/Windows 2000 Server with Service Pack 3 (minimum), Service Pack 4 or later (recommended)
- installing other third-party software
- installing Symposium Web Client software
- configuring the application server

Note: Since there are no specific guidelines or restrictions regarding the number or size of the application server partitions for Symposium Web Client, the person installing the software must determine the best hard disk configuration for the application server. For example, there can be separate partitions for the operating system, the application software, and the shared folders that are required for exporting historical reports, or everything can be installed and configured on the same partition.

Section A: Windows 2000 server

In this section

Overview	64
Symposium Web Client and replication	65
Windows 2000 Server/Advanced Server installation and configuration	67
Applying security patches to the application server	70

Overview

Introduction

Before you can install the required third-party software or the Symposium Web Client application, you must complete the following procedures:

- creating an NTFS partition as the primary partition on the application server
- installing Windows 2000 Advanced Server/Windows 2000 Server with Service Pack 3 (minimum), Service Pack 4 or later (recommended), including SMTP and IIS on the primary NTFS partition

After you install and configure Windows 2000 Advanced Server/Windows 2000 Server, refer to “Installing third-party software on the application server” on page 73 for information about installing Active Directory and Sybase Open Client.

Symposium Web Client and replication

Introduction

As an optional configuration, Symposium Web Client 4.5 application servers can exist in a replication environment where there is more than one application server running in the same domain. In this configuration, each Symposium Web Client application server in the replication environment is a domain controller within the same domain. For details on how to set up a replication environment, refer to the applicable Microsoft documentation, which can be found at http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/windows2000/techinfo/reskit/en-us/distrib/dsbh_rep_MQEG.asp (as of the date of publication).

Replication causes certain Symposium Web Client data files to be copied between replicated servers. However, not all Symposium Web Client data is replicated. The following data is replicated between servers within the same domain:

- access classes
- partitions
- private and graphical real-time reports
- real-time report filters

The data listed above is exchanged between the Symposium Web Client 4.5 application servers, so that if it is changed on one server, it is replicated to the other application servers.

No other Symposium Web Client data is replicated. The data that is not replicated includes:

- scheduling data for Contact Center Management assignments
- scheduling data for historical reports
- historical report output files
- user-created historical reports that are imported into Symposium Web Client

- real-time report exported files
- Emergency Help exported files

Notes:

- The version of the Symposium Web Client software must be the same on each server within the domain.
- When restoring data to a Symposium Web Client server that is replicated, you may need to carry out an authoritative restore. See the Microsoft documentation on Active Directory replication for more information. As of the date of publication, you can find this documentation at http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/windows2000/techinfo/reskit/en-us/distrib/dsbh_rep_jfbg.asp.
- Replication should not be used as a method of backing up Symposium Web Client data for the following two reasons:
  - Not all Symposium Web Client data is replicated.
  - You cannot use replication to roll back data to a specific time, which may be required.

  For more details on how to back up Symposium Web Client data, refer to Section D: “Backing up and restoring user data” on page 145.

ATTENTION

If you have to perform a Symposium Call Center Server platform migration, after the migration is finished, Nortel Networks recommends that you restart each Symposium Web Client application server that connects to the affected server in Symposium Call Center Server.

Windows 2000 Server/Advanced Server installation and configuration

Introduction

This section provides you with a high-level overview of the recommended configurations for Windows 2000 Advanced Server/Windows 2000 Server (with Service Pack 3 (minimum), Service Pack 4 or later [recommended]) that are specific to the Symposium Web Client application. This section is not intended to provide you with detailed procedures for installing Windows 2000 Server/ Advanced Server. For tips on installing the operating system software, see Appendix A, "Installation worksheets and checklists."

ATTENTION

When you install Symposium Web Client, the Web Client setup wizard creates a Windows 2000 Server/Advanced Server user called *iceadmin* and assigns full administrative access rights to this user. If you delete this user or modify the user's password in Windows 2000 Server/Advanced Server after you install the Symposium Web Client software, then you will not be able to log on to Symposium Web Client either as *webadmin*, or any other user. You must not change the *iceadmin* password after you install the software.

Windows 2000 Server/Advanced Server installation checklist

You can save time and effort by following the "Windows 2000 Server/Advanced Server installation checklist" on page 550. The items in this list describe the Windows 2000 Server components whose installation or configuration affect Symposium Web Client functions.

Note: This information is *not* a comprehensive walk-through of the operating system's installation process. For detailed information on Windows 2000 Server/ Advanced Server and how to install it, see the documentation that accompanies the Windows 2000 Server/Advanced Server installation CD.

Windows 2000 Server requirements

When you install Windows 2000 Server with Service Pack 3 (minimum), Service Pack 4 or later (recommended), there are several Windows components in the installation process that are required for Symposium Web Client:

- Internet Information Services (IIS) with Simple Mail Transfer Protocol (SMTP)
- Terminal Services and Terminal Services Licensing.

ATTENTION

As of date of publication, the following information on Client Access Licensing was available from Microsoft. Consult Microsoft for the latest information. Nortel Networks does not accept any liability for end-user compliance with Microsoft licensing agreements. This information has been provided for your convenience.

- You must purchase from Microsoft both a Terminal Services Client Access License and a Windows 2000 Server Client Access License for each client PC running on Windows 98 or NT that will be accessing the Script Manager portion of the Scripting component.
- Client PCs running on Windows 2000 or Windows XP require a Windows 2000 Server Client Access License only; they do not require a separate Terminal Services Client Access License.
- Nortel Networks does not provide these Client Access Licenses.
- The Windows 2000 Server Client Access Licenses do not float (that is, they are specific to the client PCs for which they have been purchased).
- If the client PC is accessing only Script Variables or Application Thresholds, then these licenses are not required.

Note: IIS and SMTP are automatically installed if you accept the default settings in the Windows Components Wizard. To install Terminal Services, you must scroll through the list of components and check the Terminal Services and Terminal Services Licensing boxes. For more information, see the “Windows 2000 Server/Advanced Server installation checklist” on page 550.

Note: Terminal Services can communicate with the Terminal Services License Server (Terminal Services Licensing) only if they are in the same domain. Therefore, Nortel Networks recommends that you install both on the application server because it is a domain controller.

Upgrading to Windows 2000 Server Service Pack 3 or later

After you install Windows 2000 Server, you must upgrade to Service Pack 3 (minimum), Service Pack 4 or later (recommended). You can download the files from Microsoft’s web site, or install the files from CD-ROM.

Applying security patches to the application server

Introduction

Given the number of operating system security patches and the complexity inherent in any network, Nortel Networks recommends that you create a systematic and accountable process for identifying and applying patches.

To help create such a process, you can follow a series of best practices guidelines, as documented in the National Institute of Standards and Technology (NIST) Special Bulletin 800-40, *Procedures for Handling Security Patches*. This bulletin suggests that if an organization does not have a centralized group to coordinate the storage, evaluation, and chronicling of security patches into a library, then system administrators or the contact center administrator must fulfill this role.

In addition to these guidelines, whenever possible, Nortel Networks recommends that you follow Microsoft's recommendations regarding newly discovered vulnerabilities and that you promptly install any security patches issued by Microsoft. Nortel Networks also recommends that you follow the security guidelines for Symposium Web Client, which are available through Nortel Networks support organizations or your distributor.

Whenever possible, Nortel Networks incorporates the latest OS security recommendations and patches in an integrated solutions testing strategy during each test cycle. However, due to the urgent nature of security patches when vulnerabilities are discovered, Nortel Networks recommends that customers follow Microsoft's guidelines as they are issued, including any Microsoft installation procedures and security patch rollback processes that may be in place. Finally, you must make a full system backup before patching the system to ensure that a rollback is possible, if required.

Note: If Symposium Web Client does not function properly after you apply a Microsoft security patch, then you must remove the patch and revert to the previous version of Symposium Web Client (from the backup you made before applying the patch). For added security, always check to see if Nortel Networks has already verified the Microsoft patch for its compatibility with Symposium

Web Client by going to the Symposium Web Client section of the Partner Information Center (PIC) web site at: https://app12.nortelnetworks.com/cgi-bin/mynn/home/NN_prodDoc.jsp?BkMg=0&prodID=24782&progSrcID=-8026&whereClause=23&curOid=12460. On this page, under the Tools section heading, click on the link for the Symposium Service Packs and Security Hotfixes Compatibility List.

What's next?

If you did not configure a DNS server during the Windows 2000 Server installation, Symposium Web Client cannot find the Symposium Call Center Server systems. In this case, your next step is to manually update the HOSTS or LMHOSTS tables. For more information, refer to "Did you configure a name resolution server?" on page 527.

If you did configure a DNS server during the Windows 2000 Server/Advanced Server installation, your next step is to install Microsoft Active Directory.

Section B: Installing third-party software on the application server

In this section

Overview 74
Installing Microsoft Active Directory 75
Installing Sybase Open Client on the application server 88

Overview

Introduction

After installing Windows 2000 Server Service Pack 3 (or later), you must install and configure Microsoft Active Directory on the application server before you install Symposium Web Client.

Also, you must install Sybase Open Client v.12.5 to use the Historical Reporting or Contact Center Management component of Web Client.

Installing Microsoft Active Directory

Introduction

Active Directory is an information storage framework used in Windows 2000 that is required to identify network components and characteristics of your network.

Active Directory is not designed to hold dynamic, constantly changing data. Information in Active Directory is data that needs to be accessed quickly, but that does not change frequently. For example, the names of users in a domain and the network printers available to those users are types of information that is constantly in demand within a domain, but that does not change often.

Note: Before you install Microsoft Active Directory, ensure that you are logged on as the Administrator or with a user name that has administrator privileges, and ensure that the computer name of the server on which you are installing Active Directory is no more than 12 characters long.

The following procedures for Active Directory installation are a guideline only. You may need to modify the installation process to meet existing requirements at your organization if you are already using Active Directory.

ATTENTION

Even if you already have a domain controller set up for your organization, make sure that you set up the Symposium Web Client application server as a domain controller for a new domain. Microsoft Active Directory's installation wizard prompts you to indicate the type of domain controller that you want to create, and allows you to create a new domain tree for Symposium Web Client. If you do not set up the application server as a separate domain, Symposium Web Client does not function properly.

To install Microsoft Active Directory

1 Click Start → Run.

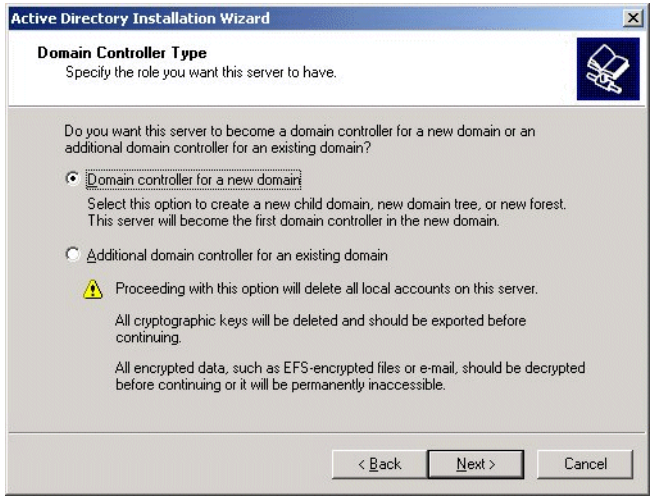
Result: The Run dialog box appears.

2 In the **Open** box, type **dcpromo** and click **OK**.

Result: The Active Directory wizard appears.

3 Click **Next**.

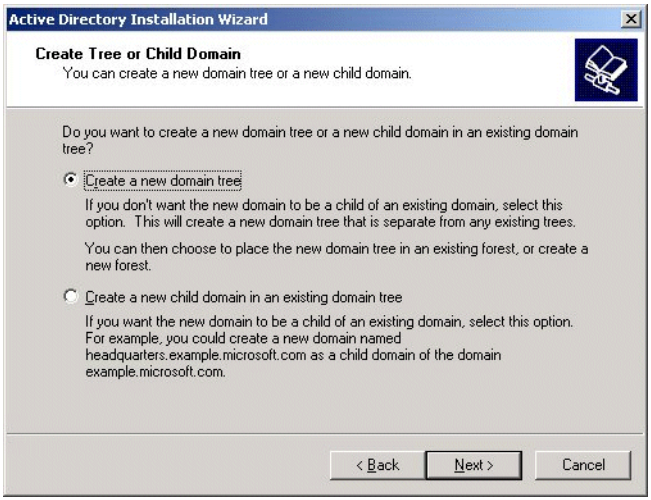
Result: The Domain Controller Type window appears.



4 Click **Domain controller for a new domain** to indicate that you are setting up the Symposium Web Client application server as the domain controller in the new domain tree (to which it will belong).

5 Click **Next**.

Result: The Create Tree or Child Domain window appears.

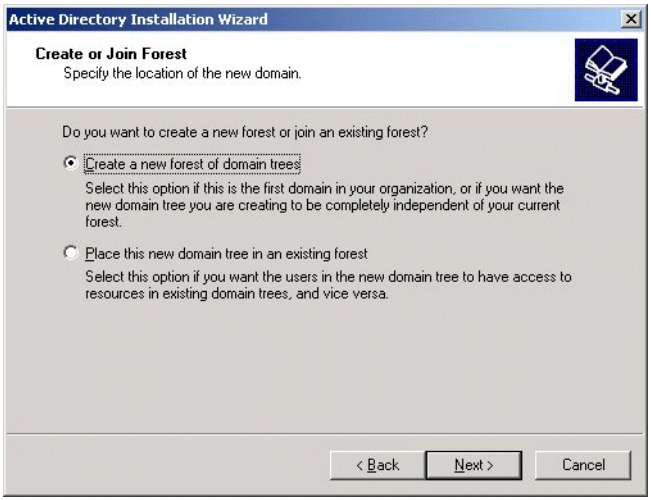


6 Click **Create a new domain tree**.

By creating a new domain tree, you ensure that the Symposium Web Client application server and any other domains that you add to the new domain tree at a later date share the same schema and configuration, and form a contiguous name space. For example, one domain can be symposium.webclient.com and another domain can be meridian.webclient.com. Both share the name space webclient.com, but are separate domain trees.

7 Click **Next**.

Result: The Create or Join Forest window appears.

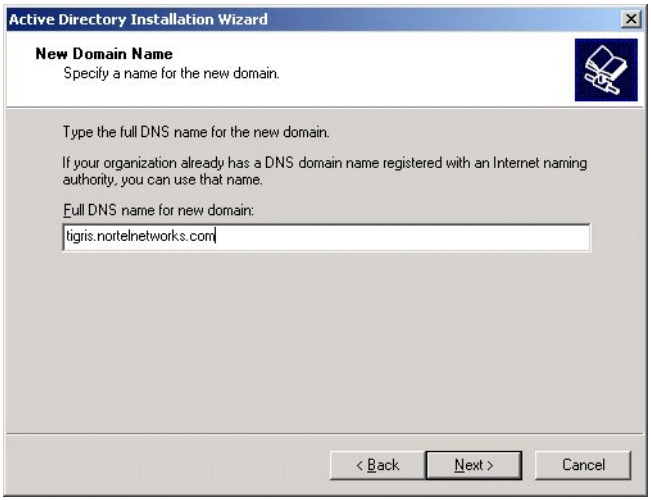


8 Click **Create a new forest of domain trees**.

By creating a new forest of domain trees, you indicate to Active Directory that you want to have multiple domain trees that share a common schema, configuration, and global catalog, but do not share a contiguous name space. For example, two domain trees (nortelnetworks.com and webclient.com) can belong to the same forest, but, with different names, do not form a contiguous name space.

9 Click **Next**.

Result: The New Domain Name window appears.



10 In the **Full DNS name for new domain** box, type <***computername*>.<*domain name*>.com** where <*computername*> is the name of the application server on which Symposium Web Client will reside, and <*domain name*> is the name of the domain tree (to which the application server will belong).

A forest is a collection of one or more Windows 2000 domains that share a common schema and global catalog. Domain trees are used to index domain names. If you have multiple domain trees that do not form a contiguous name space (for example, the two domain trees nortelnetworks.com and webclient.com), then they form separate domain trees within the forest, instead of a single domain tree. For more information on domain trees and forests, consult the Microsoft web site.

ATTENTION

If you did not install the Windows 2000 Server operating system and are unsure of the name that was assigned to this computer, open the System dialog box in Control Panel and check the Network Identification tab.

The computer name can be a maximum of 12 characters only.

Before you choose the domain name for the application server, consult with your LAN administrator to ensure that it adheres to the naming conventions established for your network. You cannot change the domain name after you install Symposium Web Client. To change the domain name, you must uninstall and reinstall the software with the new name.

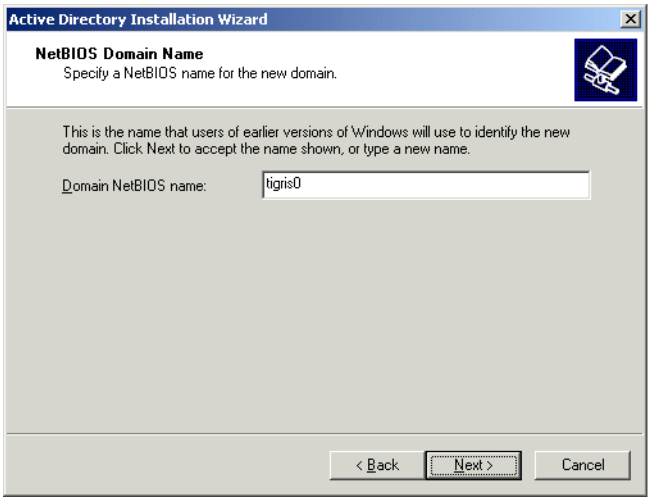
11 Click **Next**.

a. If the computer name that you entered as part of the domain name in the previous step (the name of the Web Client application server) is registered in your LAN domain controller, the Active Directory installer detects that registration and displays the following dialog box with a message indicating that the computer name that you entered has been modified slightly to resolve name conflicts on the network:

The Active Directory Installer adds a zero (0) to the computer name that you typed in the New Domain Name window. For example, if you typed “Tigris” as the domain name, Active Directory modifies it to “Tigris0” to create a new name and, therefore, resolve the name conflict.

b. Click **OK** to close the dialog box.

Result: The NetBIOS Domain Name window appears and displays a name for the NetBIOS domain. This is the computer name that you entered in the New Domain Name window.



ATTENTION

Nortel Networks recommends that you do not change the name that appears in the Domain NetBIOS name box. If Windows 2000 Server's setup discovers a name conflict, it modifies the name that you enter, adding a zero (0) at the end. Do not remove the zero from the computer name displayed in the Domain NetBIOS name box.

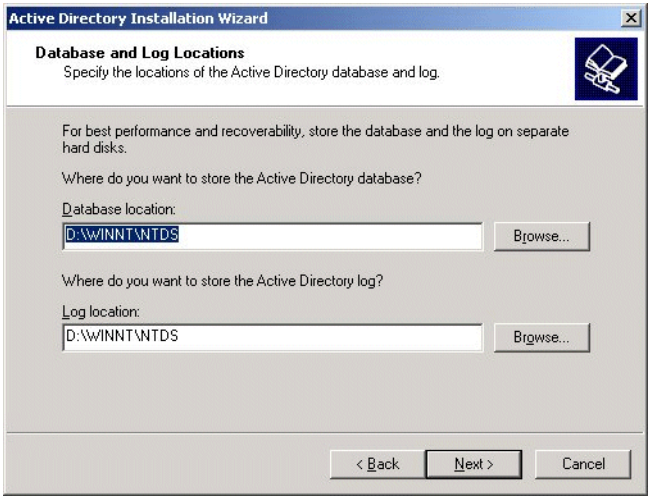
12 Click **Next**.

Result: The Database and Log Locations window appears.

13 In **Database location** and **Log location**, you can accept the defaults, type new paths, or click the **Browse** buttons and navigate to a new path for each location. The path and folder that appear in this window become the

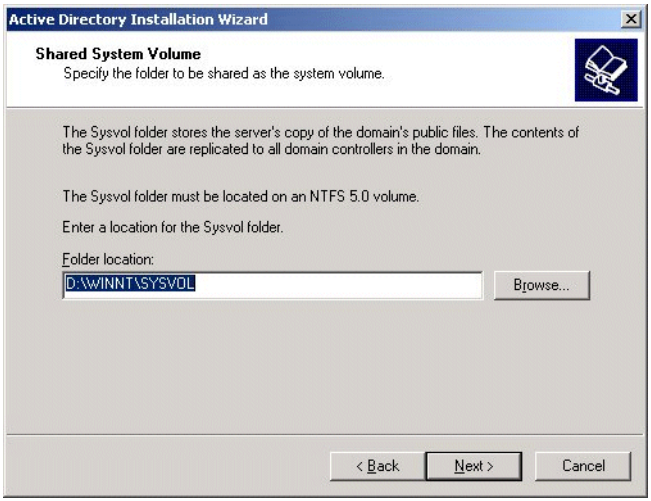
location of the Active Directory databases. Active Directory can be installed on any drive on the server, provided it has enough space.

Note: The drive letter shown in the following graphic may not match the default drive letter that appears on your server. Choose the appropriate drive and path for the Active Directory database and log.



14 Click **Next**.

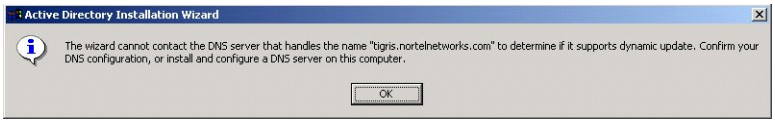
Result: The Shared System Volume window appears.



15 In **Folder location**, you can accept the default path, type a new path, or click **Browse** to navigate to a new path.

16 Click **Next**.

Result: If a dialog box appears indicating that the Active Directory Installer was unable to contact the DNS server that handles the application server, this is normal.

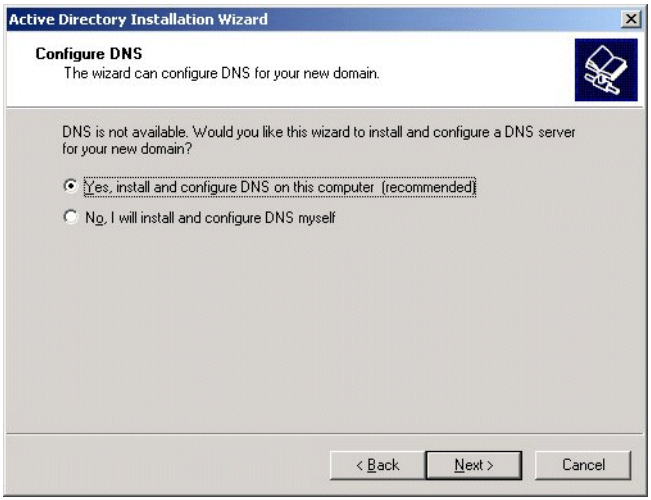


Active Directory is unable to contact the DNS server because you have just created a new computer name that is not registered in the LAN DNS.

If this dialog box does not appear, proceed to step 18.

17 Click **OK** to proceed with the installation.

Result: The Configure DNS window appears.

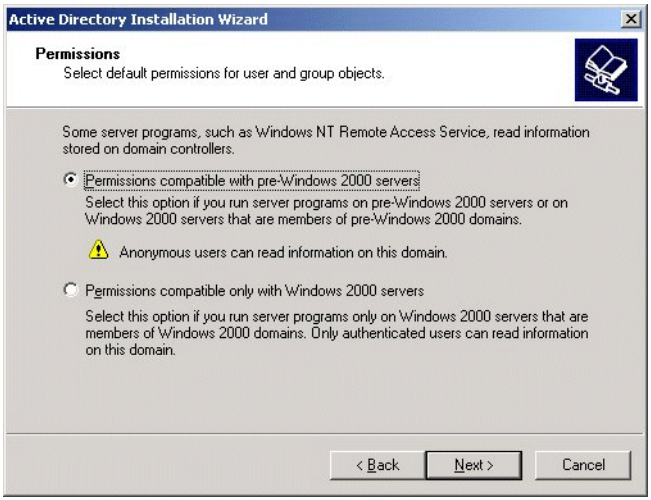


18 Click **Yes, install and configure DNS on this computer**.

Note: For proper Symposium Web Client functionality, you must select this option.

19 Click **Next**.

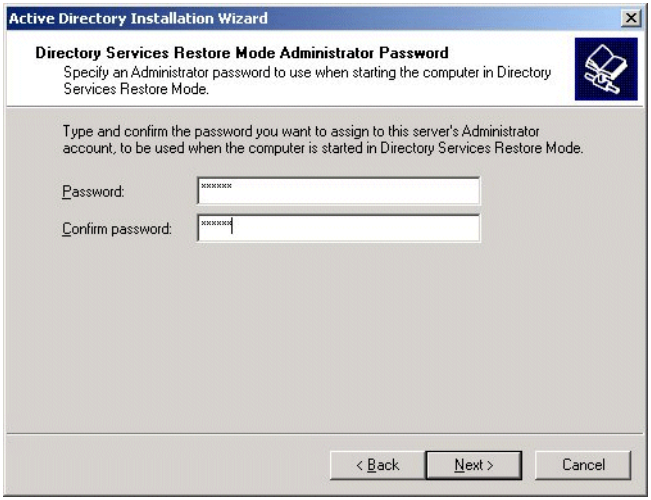
Result: The Permissions window appears.



20 Click **Permissions compatible with pre-Windows 2000 servers**.

21 Click **Next**.

Result: The Directory Services Restore Mode Administrator Password window appears.

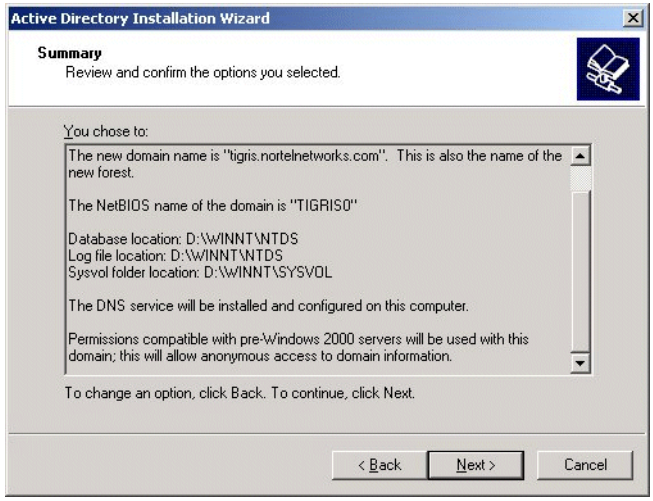


22 In the **Password** and **Confirm password** boxes, type the password for Directory Services on the application server.

Tip: Nortel Networks recommends that you use the same password for Directory Services that you use to log on to Windows 2000 Server as the Administrator.

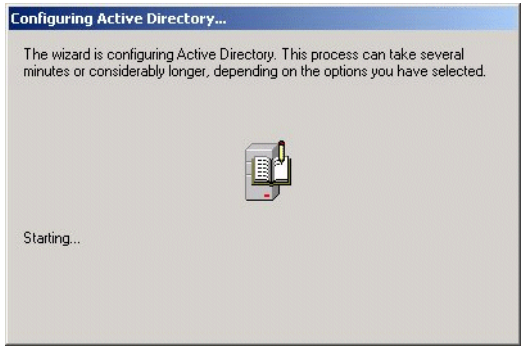
23 Click **Next**.

Result: The Summary window appears.



24 Confirm the Active Directory options listed in the Summary window, and then click **Next**.

Result: The Configuring Active Directory window appears. The system begins the installation when it completes the configuration.



Note: If you did not install and configure the DNS in 18, the **Skip DNS** button appears. Do not click this button. DNS must be installed for Web Client to function properly.

Result: When the system completes the installation, the Completing the Active Directory Installation Wizard window appears.

25 Click **Finish**.

Result: The Active Directory Installation Wizard's restart dialog box appears.

26 Click **Restart Now**.

Result: The system restarts.

What's next?

Install Sybase Open Client, and then install Symposium Web Client.

Note: You must have the Symposium Web Client CD-ROM on hand for these next two procedures.

Installing Sybase Open Client on the application server

Introduction

You must install Sybase Open Client v.12.5 to use the Historical Reporting and Contact Center Management components. To install Sybase Open Client, you must have administrator privileges on the application server.

Note: If you have Sybase v.12.0 installed on the application server, then you can perform an upgrade to Sybase v.12.5 using the following procedure. If you have a version of Sybase earlier than 12.0 installed on the application server, then you must uninstall it before you install version 12.5. For information on uninstalling the software, see the documentation posted on the Sybase web site at http://manuals.sybase.com/onlinebooks/group-as/asp1200e/aseinsnt.

After you install Sybase Open Client Version 12.5, you must update the Sybase Open Client driver. For details, see “To upgrade the Sybase 12.5 ODBC driver” on page 92.

To verify the version of Sybase Open Client that is already installed

If the server already has Sybase Open Client installed, perform the following procedure to verify the version of the software before upgrading to Sybase Open Client 12.5:

1. On the server, Start → Settings → Control Panel.
2. Click **System**.

   Result: The System Properties window appears.
3. Click the **Advanced** tab.
4. Click **Environment Variables**.

   Result: The Environment Variables window appears.
5. Within the System variables section, locate the Sybase software entries. For example, if Sybase Open Client Version 12.0 is installed on the server, it says *SYBASE_OCS: OCS_12_0*, and for Sybase Open Client Version 12.5, it says *SYBASE_OCS: OCS_12_5*.

To install Sybase Open Client

You can use this procedure to install Sybase Open Client v.12.5 for the first time, or to upgrade from v.12.0.

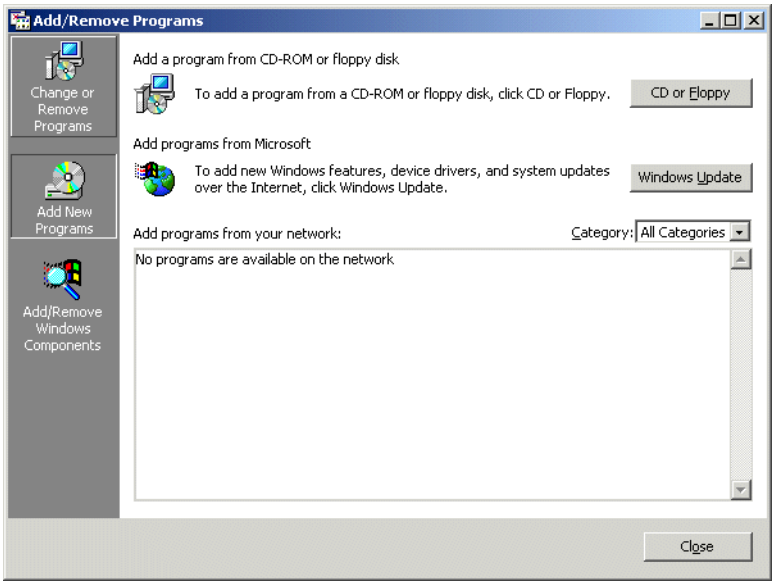
Symposium Web Client only functions with Sybase Open Client 12.5. If the application server already has a version of Sybase installed that is *newer* than version 12.5, then you must uninstall it completely before installing version 12.5. For information on uninstalling Sybase software, see the Sybase documentation.

Tip: Insert the Symposium Call Center Web Client CD in the CD-ROM drive.

1 Click Start → Settings → Control Panel.

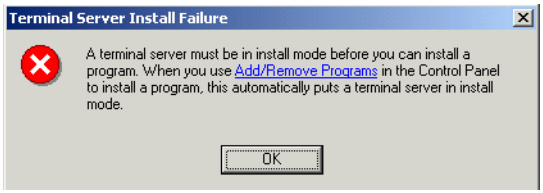
2 Double-click **Add/Remove Programs**.

Result: The Add/Remove Programs window appears.



Note: If you double-clicked the Sybase Open Client v.12.5 setup.exe file on the Symposium Web Client CD, or if the setup file launched automatically, the Terminal Server Install Failure dialog box appears. This occurs because

Terminal Services must be in Install Mode before you can install an application.



To switch Terminal Services to Install Mode, select the Add/Remove Programs link in the dialog box. The Add/Remove Programs window appears, and Terminal Services automatically switches to Install Mode.

3 Click **Add New Programs**.

4 Click **CD or Floppy** to indicate that you want to install Sybase Open Client from the CD-ROM.

Result: The Install Program From Floppy Disk or CD-ROM window appears.

5 Click **Next**.

Result: The Run Installation Program window appears.

6 Click **Browse** and navigate to the Sybase folder on the CD-ROM: D:\SYBASE, where D:\ is the CD-ROM drive.

7 Double-click **setup.exe**.

Result: The path to the setup.exe file appears in the **Open** box.

8 Click **Next**.

Result: The Sybase Installer window appears, followed by the Installation Type window.

9 Click **Standard Install**, and then click **Next**.

Result: The Choose Directory window appears.

10 If you are installing the software for the first time, type a custom location in which to install the software, or accept the default location shown. Nortel Networks recommends that when you are upgrading from Sybase 12.0, you choose the same folder in which the Sybase software is currently installed. However, if you do not know this location, then you can type a custom

location in which to install the software, or accept the default location shown (C:\SYBASE).

ATTENTION

When choosing a custom location in which to install the Sybase software, do not choose a directory name that contains a space. For example, do *not* choose *D:\Program Files\Sybase* because the Sybase installation program cannot process the space in "Program Files."

11 Click **Next**.

Result: The Summary window appears, displaying the components being installed.

12 Click **Next**.

Result: The Create Directory window appears, prompting you to confirm the name of the directory to which the files will be copied.

13 Click **Yes**.

Result: The Installing window appears, displaying a status bar while the system installs the program. If you are upgrading to Sybase v.12.5, the system asks if you want to overwrite the following existing *Sybase* .DLL files. Click **Yes** when prompted to replace/reinstall these Sybase files:

- replace mchelp.dll Version 12.0 with Version 12.5.0.0
- replace mclib.dll Version 12.0 with Version 12.5.0.0
- replace Language Modules version 12.0 with Version 12.5
- reinstall Component Sybase Central 3.2.0

If the system prompts you to replace the following optional file, you can click either **Yes** or **No**. Since the file is optional, your choice does not affect the Sybase installation:

- replace Power Dynamo Version 3.0.0 with Version 3.5.2

If the system prompts you to replace any other DLLs, including *system* DLLs, such as msvcrt40.dll Version 4.20, click **No**. Do not replace any system DLLs.

Note: If a window with the following message appears, click **OK**: *COMCTL32.DLL - The system does not need this update.*

When the installation is complete, the Sybase Installer window appears, prompting you to restart the system before configuring the installed components.

14 Click **Yes**.

Result: This can take several minutes. Do not attempt to manually restart the system. When restarting, log on as a user with administrator privileges. After the system restarts, the Information window appears, confirming the Sybase installation.

ATTENTION

Do not remove the Symposium Web Client CD from the CD-ROM drive during the system restart process. The Installation Wizard carries out some final configuration procedures after the system restarts.

15 Click **OK**.

16 Close the Control Panel window. Continue with the following procedure, "To upgrade the Sybase 12.5 ODBC driver" on page 92.

To upgrade the Sybase 12.5 ODBC driver

After you install Sybase Open Client Version 12.5, you must perform the following procedure to update the Sybase ODBC driver, EBF11113.

1 On the application server, free up all active Sybase Open Client connections as follows:

a. Close all Symposium Web Client browser sessions.

b. Stop any other third-party applications that are running on the application server and that use Sybase Open Client.

2 On the application server, reset IIS as follows:

a. Click Start → Run.

b. In the **Open** box, type *iisreset*, and then click **OK**.

3 Install the updated driver, EBF11113, as follows:

a. On the application server, open an MS-DOS prompt, and then navigate to the root directory of the Symposium Web Client CD-ROM.

b. Type the following xcopy command:

copy EBF11113.* %SYBASE% /s /e /v /Y > C:\EBF11113.TXT*

In this command, *EBF11113* is the directory containing the Sybase ODBC driver, *%SYBASE%* is the environment variable containing the directory location of Sybase Open Client 12.5 software installed on the application server, and *C:\EBF11113.TXT* is the log file that you can use to verify if all the files were copied correctly.

4 On the application server, verify that the system successfully updated the driver as follows:

a. Click Start → Programs → Administrative Tools.

b. Click the Data Sources (ODBC) icon.

Result: The ODBC Data Source Administrator window appears.

c. Click the **Drivers** tab.

d. In the tab, scroll down until you locate the Sybase ASE ODBC driver. The correct driver version is 4.10.00.49.

Note: If the ODBC driver version is not 4.10.00.49, then open the log file, C:\EBF11113.txt, to verify if there were any error messages recorded during the xcopy.

What's next?

Install Symposium Web Client.

Section C: Installing Symposium Web Client on the application server

In this section

Overview 96

Installing Symposium Web Client on the application server 98

Installing or repairing individual Symposium Web Client components on the application server 116

Uninstalling application server software 122

Configuring multiple-language support 128

Configuring multiple language support in Agent Desktop Displays 143

Overview

Introduction

The following steps detail how to install and configure Symposium Web Client. The Web Client installation wizard requires approximately 5 minutes to acquire configuration information and to perform the installation.

Before you begin, check for updates in any installation addenda posted on the appropriate web site:

- http://www.nortelnetworks.com (for end customers)
- http://www.nortelnetworks.com/prd/picinfo/ (for distributors)

Minimum requirements

Note: The system requirements and installation procedures apply to Symposium Web Client and the Symposium Configuration Tool.

Before you install and use Symposium Web Client, you must ensure that the following Windows components and third-party software have been installed and configured on the application server:

- Windows 2000 Server Service Pack 3 or later, or Windows 2000 Advanced Server, Service Pack 3 or later
- Internet Information Services with SMTP
- Microsoft Active Directory
- Terminal Services and Terminal Services Licensing (required only for the Script Editor portion of the Scripting component)
- Sybase Open Client v.12.5 (required for Historical Reporting and Contact Center Management)
- Windows Installer 2.0 or later (version 2.0 is included on the Symposium Web Client CD-ROM, and in both Windows 2000 Service Pack 3 for Windows 2000 Server and Professional, and Windows XP)

If the Symposium Web Client setup wizard does not detect these programs or components on the application server, it terminates the installation process.

Before you install Symposium Web Client, you must decide if you are installing Symposium Web Client as the default web site on the application server, or if you are installing it as a virtual directory on an existing web site. See “Web sites and virtual directories” on page 576 for more information on how to determine the type of web site that best suits your company’s needs.

ATTENTION

Nortel Networks recommends that you install Symposium Web Client as the default web site, reserving the application server solely for the use of Symposium Web Client.

Installing Symposium Web Client on the application server

Introduction

You must have administrator privileges in Windows 2000 Server to install Symposium Web Client. After you install the software from the Symposium Web Client CD, apply the latest Service Update from the applicable Nortel Networks MPL web site (from https://www21.nortelnetworks.com/MPL for Europe, or https://www43.nortelnetworks.com/MPL for North America). Service updates are no longer supplied on a supplementary CD for Symposium Web Client.

Note: To register for either of these web sites, follow the instructions listed at http://nortelnetworks.com/register.

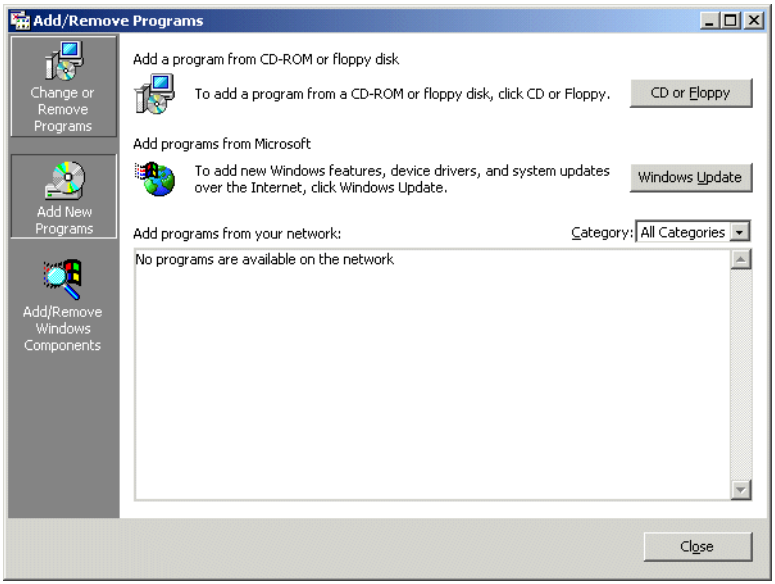
To install Symposium Web Client on the application server

1 Insert the Symposium Web Client CD in the CD-ROM drive.

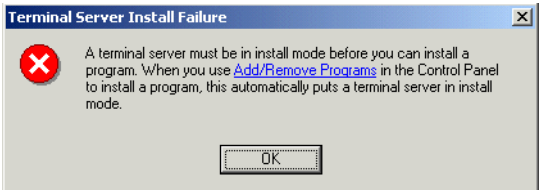
2 Click Start → Settings → Control Panel.

3 Double-click **Add/Remove Programs**.

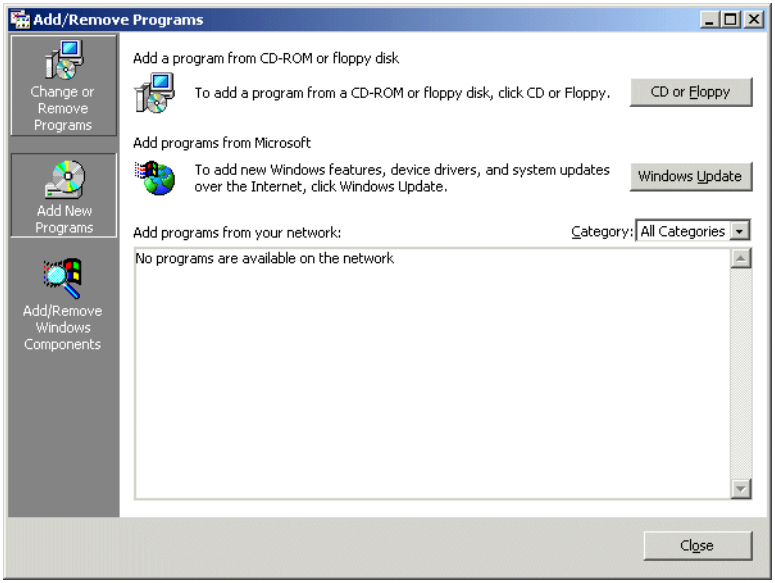
Result: The Add/Remove Programs window appears.



Note: If you double-clicked the Symposium Web Client setup.exe file on the Symposium Web Client CD, or if the setup file launched automatically, the Terminal Services Install Failure dialog box appears. This occurs because Terminal Services must be in Install Mode before you can install an application.



To switch Terminal Services to Install Mode and install Symposium Web Client, select the Add/Remove Programs link in the dialog box. The Add/Remove Programs window appears, and Terminal Services automatically switches to Install Mode.



4 Click **Add New Programs**.

5 Click **CD or Floppy** to indicate that you want to install Symposium Web Client from the CD-ROM.

Result: The Install Program From Floppy Disk or CD-ROM window appears.

6 Click **Next**.

Result: The Run Installation Program window appears, and D:\setup appears by default in the Open box, where D: is the CD-ROM drive.

7 Click **Next**.

Note: The program checks to see if the required third-party software is installed on the server and stops the installation if any of the minimum requirements listed on page 96 are not met. If all requirements are met, then the installation continues (see page 101 for further steps). For example, if you do not have the Windows Installer version 2.0 or later, the program stops the installation and notifies you that you must install it before

installing Symposium Web Client. In this case, perform the following procedure.

To install Windows Installer 2.0 or later

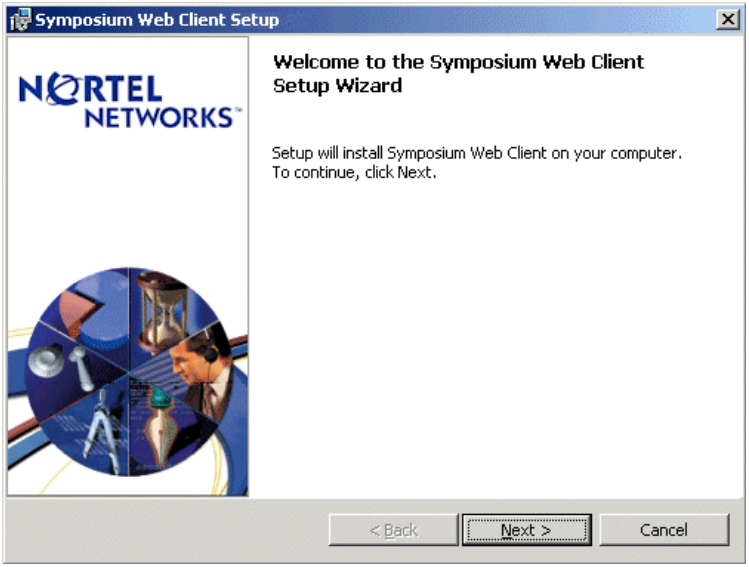
a. In the root directory of the Symposium Web Client CD-ROM, locate the folder Windows Installer 2.0 for <*your operating system*>.

b. Inside the appropriate folder, double-click the file **InstMsiW.exe**. The program installs the Windows Installer 2.0 and tells you to restart the computer when it is finished.

c. Restart the computer.

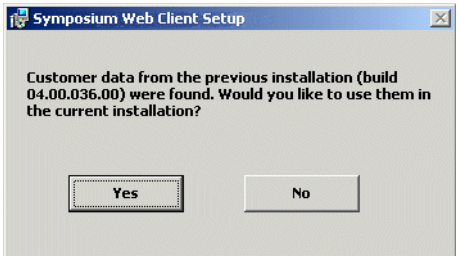
d. When the computer has restarted, if you are currently on the application server, then return to step 1 on page 98 to install Symposium Web Client. If you have just used this procedure to install the Windows Installer on the client PC, then proceed with configuring the client PC.

Result: The Symposium Web Client Setup Wizard window appears.



8 Click **Next**.

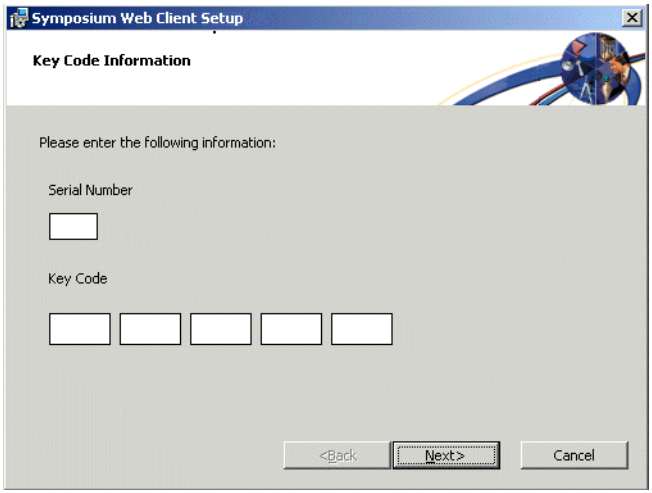
Result: If you are *reinstalling* Symposium Web Client, the system prompts you to restore customer data.



a. Click **Yes** if you want to restore previously saved data.

b. Click **No** if you do not want the system to restore previously saved data. The system does not restore the data, but it does not delete the data from the application server. The data remains in a temporary folder on the application server.

Result: The Key Code Information window appears.



9 Type the serial number and key code for your Symposium Web Client 4.5 application.

Note: The serial number is the switch ID (M1/CSE 1000) or dongle ID (DMS/MSL-100).

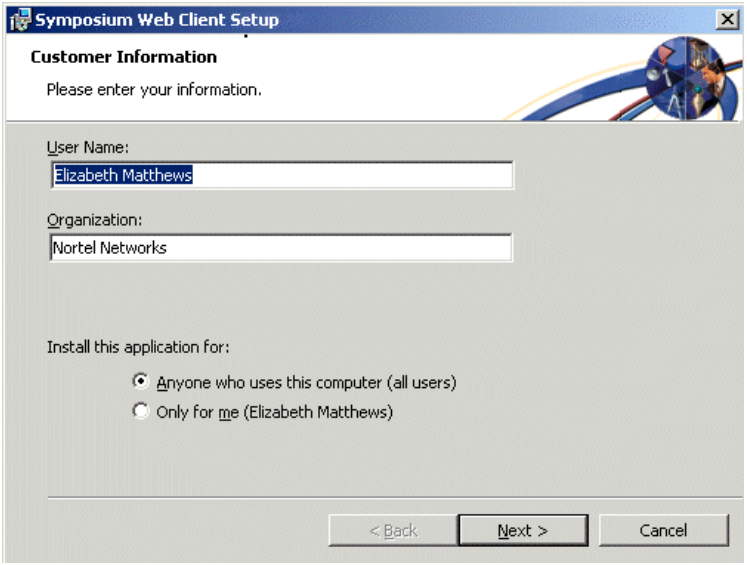
ATTENTION

Key codes are case-sensitive.

10 Click **Next**.

Note: If you made an error entering the key code or serial number, the system displays an error message in a dialog box. Click **Back** to return to the Key Code Information window, and reenter the information.

Result: The Customer Information window appears.



a. In the **User Name** and **Organization** boxes, type the appropriate information.

b. To set up access restrictions for this Symposium Web Client installation, click one of the options in the **Install this application for** section.

Anyone who uses this computer (all users) indicates that you want anyone who can log on to the computer to also be able to log on to Symposium Web Client.

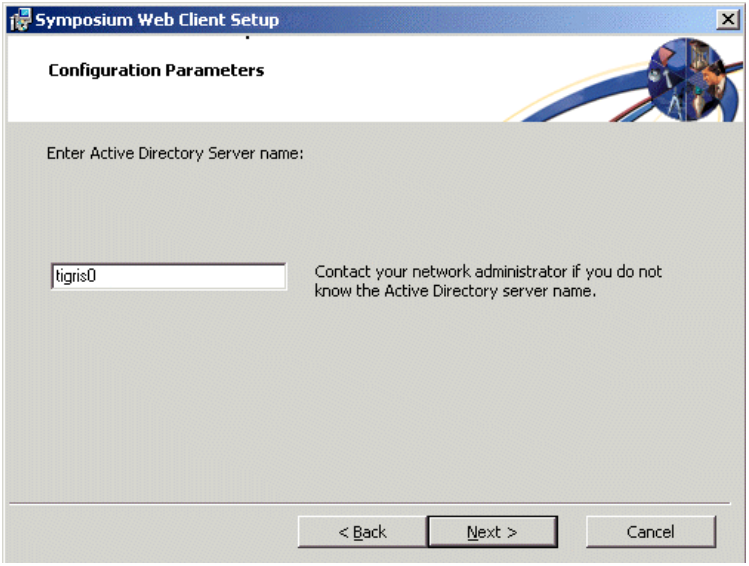
ATTENTION

Nortel Networks recommends that you click **Anyone who uses this computer (all users)**. Failure to do so can prevent users who have authorization to use Symposium Web Client from using the application server when they need to.

Only for me (<*username*>) indicates that you want to make sure that only a user with your user name and password can log on to Symposium Web Client.

11 Click **Next**.

Result: The Configuration Parameters window appears.



12 In the **Enter Active Directory Server name** box, accept the default name of the Active Directory server.

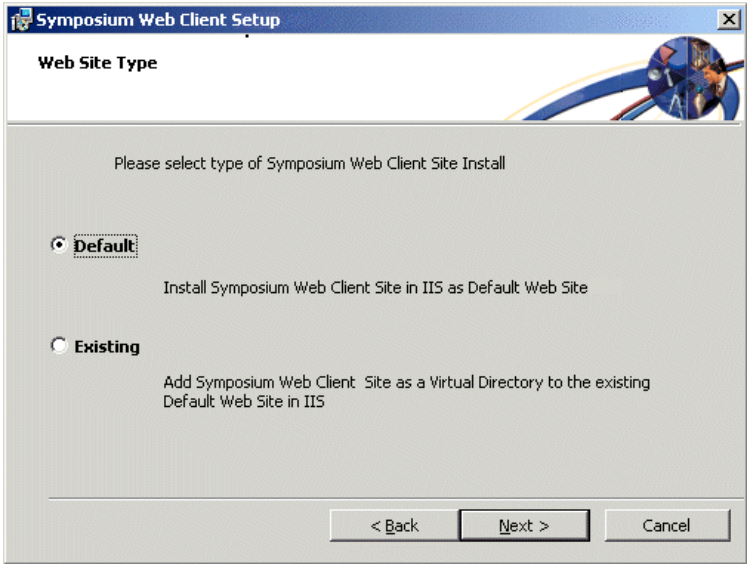
ATTENTION

Do not change this default name.

This is the NetBIOS Domain name that was provided when Active Directory was installed on the application server. For more information, see “Installing Microsoft Active Directory” on page 75.
If the default name that appears in the **Enter Active Directory Server name** box is different from the NetBIOS Domain name, an error message appears, indicating that you must ensure these two computer names are the same before the installation can continue.

13 Click **Next**.

Result: The Web Site Type window appears.



You can install Symposium Web Client as the default web site on the application server, or install it as a virtual directory on an existing web site. For more information on how to determine the type of web site that best suits your company’s needs, see “Web sites and virtual directories” on page 576.

To install Web Client as the default web site

a. Click **Default**.

ATTENTION

Nortel Networks recommends that you click **Default**, reserving the application server solely for the use of Symposium Web Client for optimum performance.

To install Web Client as a virtual directory on an existing web site

a. Click **Existing**.

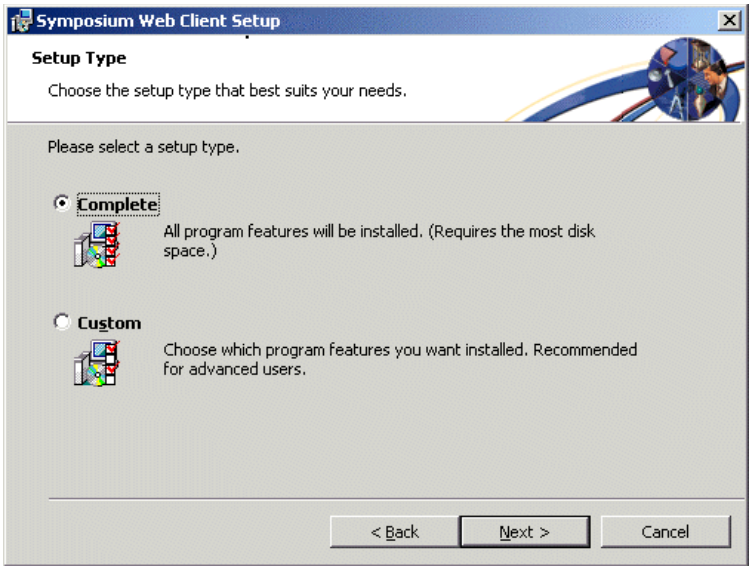
b. Click **Next**.

Result: The Virtual Directory Name window appears with *WClient* as the default name. If you want to change the name, type a new name.

Note: The name you choose will be the name of the folder in the Default Web Site tree in IIS. To see a sample of Symposium Web Client as a virtual directory and as a default web site, see “Web sites and virtual directories” on page 576.

14 Click **Next**.

Result: The Setup Type window appears.



15 Select one of the following setup types:

Complete: Click **Complete** to install all Symposium Web Client components and proceed to 19.

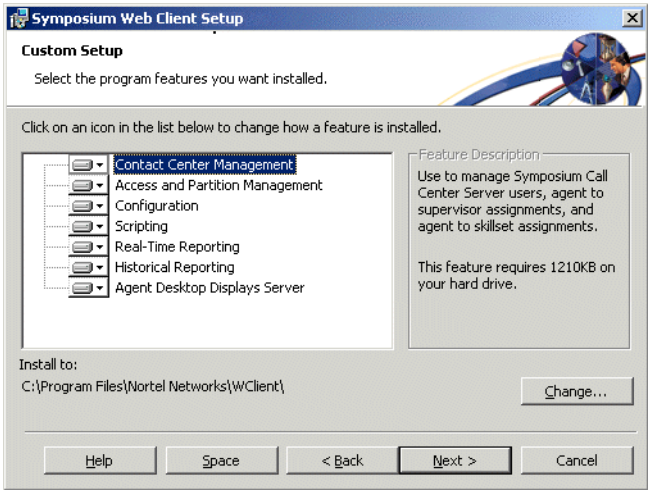
Custom: Click **Custom** to use the Custom Setup window to select which Symposium Web Client components the system will install, to change the default installation directory, or to confirm available hard disk space.

16 If you want to change the components to be installed, perform the following steps:

a. Click **Custom** in the Setup Type window.

b. Click **Next**.

Result: The Custom Setup window appears.



c. Click the icon for the component (for example, Historical Reports) that you do not want to install.

Result: A pop-up menu appears.

d. Click **This feature will not be Available**.

Result: An X appears beside the name of the component.

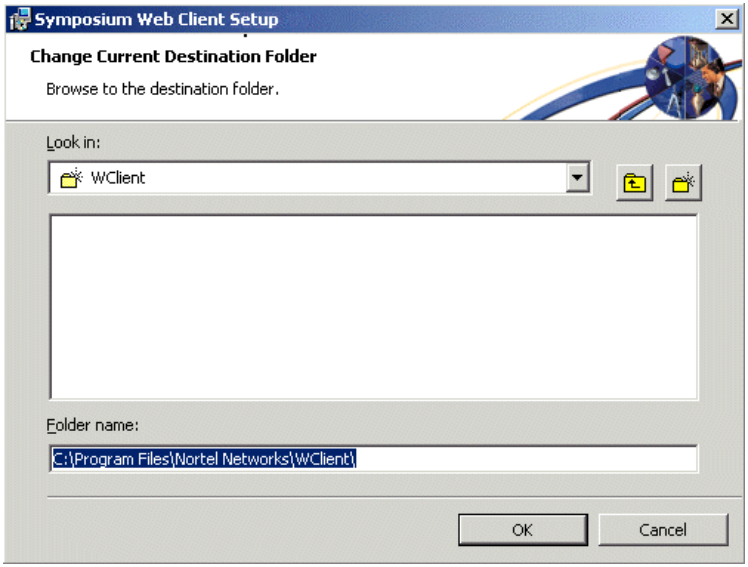
Note: Configuration, Access Management, Scripting, and Contact Center Management are mandatory for every installation of Symposium Web Client. All other components are optional. To use Agent Desktop Displays on a client, you must install the Agent Desktop Displays Server component on the application server. However, to install the Agent Desktop Displays

server component, you must first install the Real-Time Reporting component on the application server.

17 Confirm the default directory path that appears in the bottom left side of the window (when you click a component that is going to be installed). If you want to change the default directory path, perform the following steps:

a. In the Custom Setup window, click **Change**.

Result: The Change Current Destination Folder window appears.



b. In the **Folder name** box, type the path to the directory and the directory name, or navigate to the drive and directory in which you want to install the program.

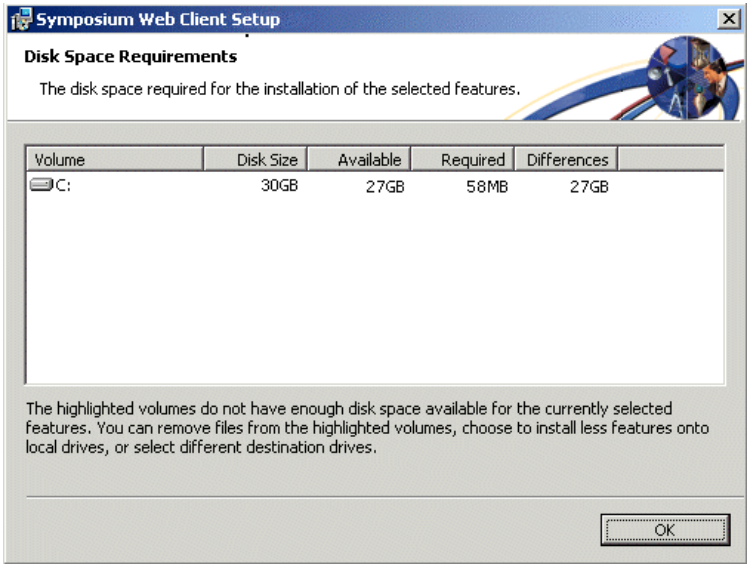
c. Click **OK** to return to the Custom Setup window.

18 If you want to confirm your available hard disk space, perform the following steps:

a. In the Custom Setup window, click **Space**.

Result: The Disk Space Requirements window appears.

Note: The Disk Space Requirements window appears automatically if you attempt to install Symposium Web Client to a drive that does not have enough free disk space.

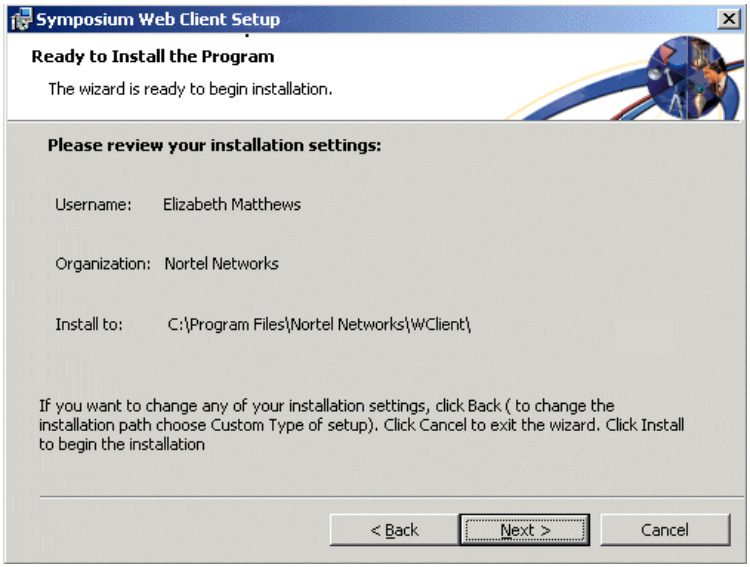


b. Review the available disk drive space and the amount of space required to install the individual components, and then click **OK** to return to the Custom Setup window.

Note: The Symposium Web Client application requires from 60 to 80 Mbytes of hard disk space (a value that varies based on the number of system files that need to be installed on your application server); however, if you are installing the Historical Reporting component, you need an additional 230 Mbytes for Crystal Reports templates.

19 Click **Next**.

Result: The Ready to Install the Program window appears.

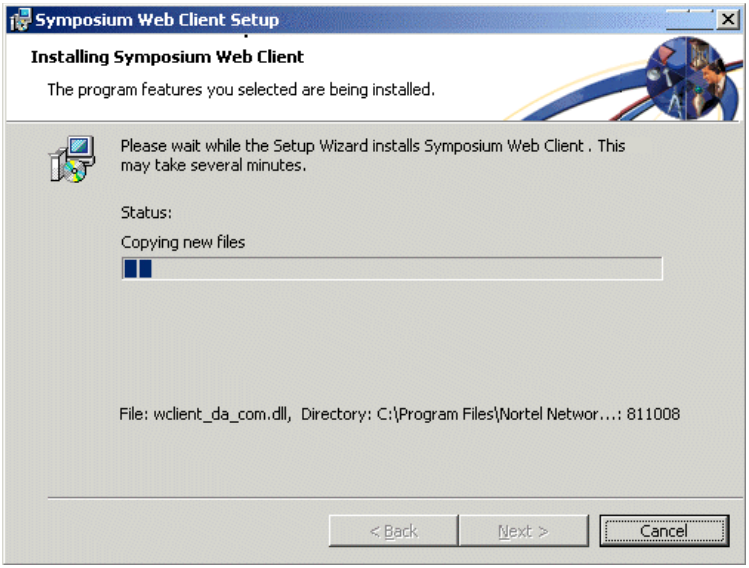


20 Click **Next**.

ATTENTION

Installation ends if you did not install the required third-party applications prior to installing Symposium Web Client.
An error dialog box appears listing the missing software, and the setup wizard closes. You cannot complete the Symposium Web Client installation until you install all required software.

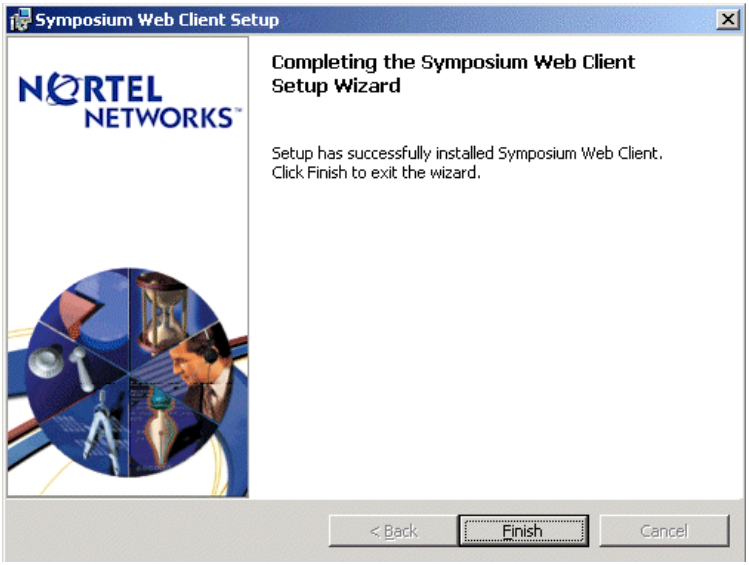
Result: The Installing Symposium Web Client window appears.



Note: Sometimes the Files in Use window appears, notifying you of files that you are using or windows that you have open that are preventing the Symposium Web Client installation from proceeding. For example, sometimes the window notifies you that you must close the Add/Remove Programs window. To continue with the installation, close the files or windows listed, and then click **Retry.** The installation proceeds.

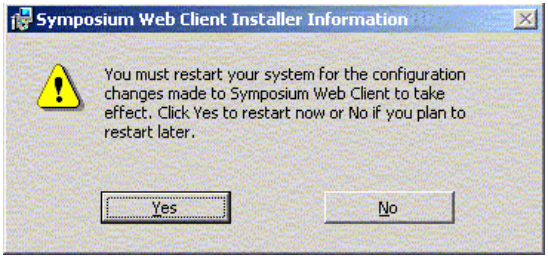
21 The program searches for installed components, and then installs the required Simple Object Access Protocol (SOAP) files.

Result: When it is finished installing all components, the Completing the Symposium Web Client Setup Wizard window appears.



22 Click **Finish** to exit the setup wizard.

Result: The Symposium Web Client Installer Information dialog box appears.



23 Click **Yes** to restart your computer.

What's next?

Download and apply the latest Service Update from https://www21.nortelnetworks.com/MPL (for Europe), or from https://www43.nortelnetworks.com/MPL (for North America). To register for either of these web sites, follow the instructions listed at http://nortelnetworks.com/register.

Optionally, you can now install the XML automated assignments feature, which is used in conjunction with the Contact Center Management component. This feature enables you to simultaneously update multiple supervisor and skillset assignments by creating a specially formatted XML file. For information on installing this feature, see the *XML Assignments User Guide*. This guide, and other associated documentation and engineering/development support resources for the XML automated assignments feature, are provided only through the Nortel Networks Developer Program.

For information on obtaining the XML Automated Assignment toolkit, contact a member of the Developer Program through the Contact Us link on their web site at http://www.nortelnetworks.com/developer. General information on the Developer Program, including an online membership application, is also available on this site.

Note: For overview information and details on using the XML automated assignments feature, see "Using the XML automated assignments feature" on page 426.

If you do not want to install this feature, then proceed directly to upgrading Internet Explorer and configuring Symposium Web Client on the application server. For more information, see "Upgrading Internet Explorer on the application server" below.

Upgrading Internet Explorer on the application server

You must upgrade the version of Internet Explorer that installs by default with Windows 2000 Server from Version 5.0 to Version 5.5 Service Pack 2 (or later) so support personnel can access the application server.

Note: The following procedure outlines how to upgrade Internet Explorer through the Microsoft utility on the Internet. When you perform this procedure, the utility enables you to upgrade only to Internet Explorer version 6.0 Service Pack 1 (or later). While you can still run Symposium Web Client on Internet Explorer version 5.5 Service Pack 2, you can only upgrade to this version if you have the software saved on CD-ROM.

To upgrade Internet Explorer on the application server

1 Open Internet Explorer and, on the menu, click Help → About Internet Explorer.

Result: The About Internet Explorer window appears.

2 Click **Update Information**.

Result: The Internet Explorer High Encryption Pack window appears in the browser.

3 In the **Search** box, type **Internet Explorer 6.0**.

4 Click **Search**.

Result: The Search Results window appears.

5 Click the latest Internet Explorer 6.0 Service Pack.

Result: The Internet Explorer 6.0 Service Pack and Internet Tools window appears.

6 Select the language version of your choice, and then click **Download Now**.

Result: The File Download dialog box appears with the **Save this program to disk** radio button selected by default.

7 Click **OK** and save the ie6setup.exe file to the folder of your choice.

Note: You cannot run the ie6setup.exe file from the web site when upgrading the application server. You must save the file on the application server's hard disk.

8 Click Start → Settings → Control Panel.

Result: The Control Panel window appears.

9 Double-click **Add/Remove** programs.

Result: The Add/Remove programs window appears.

10 Double-click **Add New Programs**.

Result: The Add New Programs window appears.

11 Click **CD or Floppy**.

Result: The Install Program From Floppy Disk or CD-ROM window appears.

12 Click **Next**.

Result: The Run Installation Program window appears.

13 Click Browse and navigate to the folder in which you saved the ie5setup.exe file that you downloaded from the Microsoft web site.

14 Click **ie6setup.exe**, and then click **Open**.

Result: The Run Installation Program window reappears with the path to the ie6setup.exe file in the Open text box.

15 Click **Next**.

Result: The Welcome to Setup for Internet Explorer and Internet Tools window appears.

16 Click **I accept the agreement**, and then click **Next**.

Result: The Initializing Setup window appears briefly and is replaced by the Windows Update: Internet Explorer and Internet Tools window.

17 Click **Next**.

Result: The Download Sites window appears.

18 Select the region from which Windows should get any additional files required for Service Pack 1, and then click **Next**.

Result: The Progress window appears and the installation begins. When the installation is complete, the Restart Computer window appears.

19 Click **Finish** to restart your system.

What's next?

Your next step is to configure Internet Explorer. For more information, refer to "Installing and configuring the browser on a client workstation" on page 292.

Installing or repairing individual Symposium Web Client components on the application server

Introduction

You can repair corrupted files for a component in Symposium Web Client by reinstalling that particular component. You can also add new Symposium Web Client components after the initial installation.

Repairing a damaged Symposium Web Client component

You can repair a damaged Symposium Web Client component, using the Add/Remove Programs feature in Windows.

To repair a damaged Symposium Web Client component

1. Insert the Symposium Web Client CD in the CD-ROM drive.
2. Click Start → Settings → Control Panel.
3. Double-click **Add/Remove Programs**.

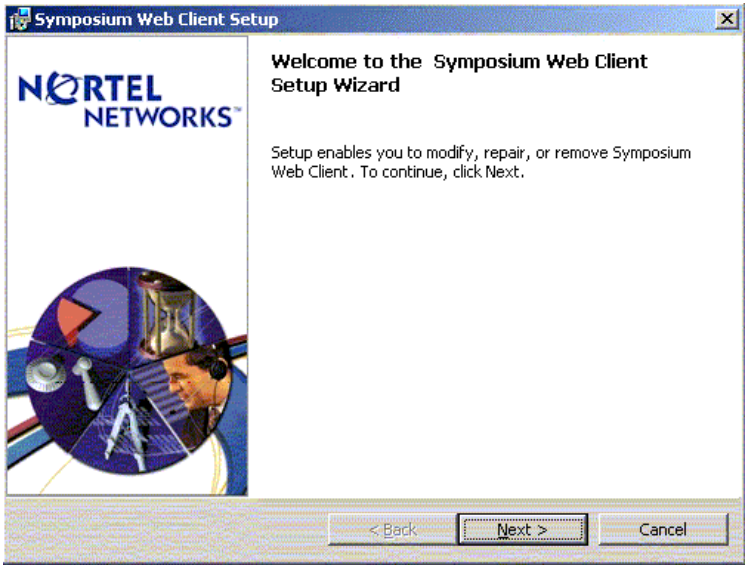
   Result: The Add/Remove Programs window appears.

   Note: If you double-clicked the Symposium Web Client setup.exe file on the Symposium Web Client CD, or if the setup file launched automatically, the Terminal Services Install Failure dialog box appears. This occurs because Terminal Services must be in Install Mode before you can install an application.

   To switch Terminal Services to Install Mode and install Active Directory, select the Add/Remove Programs link in the dialog box. The Add/Remove Programs window appears, and Terminal Services automatically switches to Install Mode.
4. Select Symposium Web Client from the list of installed programs.

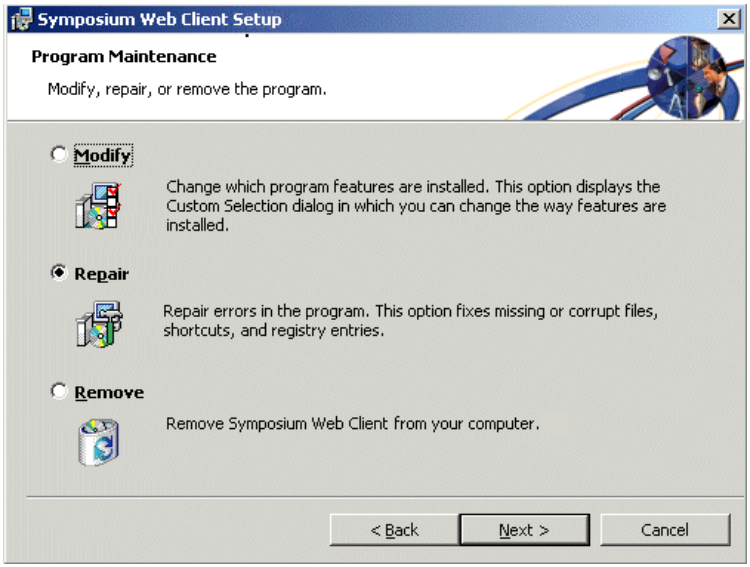
5 Click **Change**.

Result: The Welcome to the Symposium Web Client Setup Wizard window appears.



6 Click **Next**.

Result: The Program Maintenance window appears.



7 Click **Repair**.

8 Click **Next**.

Result: The Ready to Repair the Program window appears.

Note: You do not have to identify which components are malfunctioning. Symposium Web Client checks all of its components to identify those that require repair.

9 Click **Next**.

Result: The Repair window appears and the repair process begins. A repair completion message appears when the repair is finished.

10 Click **Finish** to close the Repair window.

Result: The Symposium Web Client Installer Information dialog box prompts you to restart your computer.

11 Click **Yes** to restart the system.

Installing an individual Symposium Web Client component

To install Real-Time Reporting, Historical Reporting, or Agent Desktop Displays in Symposium Web Client, run the Symposium Web Client installation program, enter a new keycode, and then install the component.

After you add the Historical Reporting component, you must install and configure Simple Mail Transfer Protocol (SMTP) on the application server if you want to take advantage of Historical Reporting's e-mail notification feature. See "To configure the SMTP server" on page 176.

To install an individual Symposium Web Client component

1. Insert the Symposium Web Client CD in the application server's CD-ROM drive.
2. Click Start → Settings → Control Panel.
3. Double-click **Add/Remove Programs**.

   Result: The Add/Remove Programs window appears.

   Note: If you double-clicked the Symposium Web Client setup.exe file on the Symposium Web Client CD, or if the setup file launched automatically, the Terminal Services Install Failure dialog box appears. This occurs because Terminal Services must be in Install Mode before you can install an application.

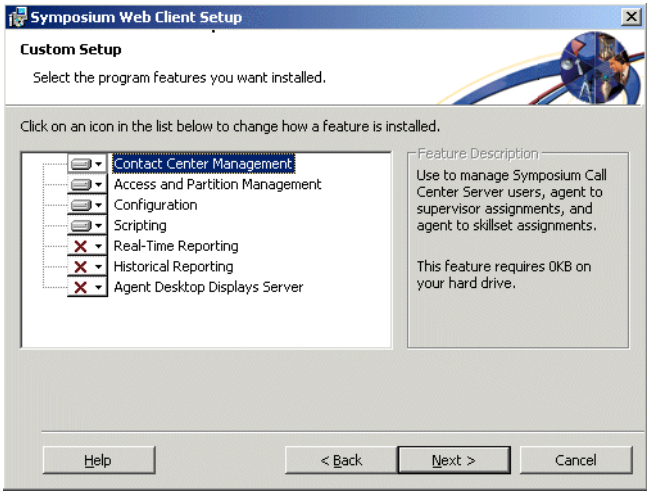
   To switch Terminal Services to Install Mode and install Active Directory, select the Add/Remove Programs link in the dialog box. The Add/Remove Programs window appears, and Terminal Services automatically switches to Install Mode.
4. Select Symposium Web Client from the list of installed programs.
5. Click **Change**.

   Result: The Welcome to the Symposium Call Center Web Client Setup window appears.
6. Click **Next**.

   Result: The Program Maintenance window appears with the system default as **Modify**.

7 Click **Next**.

Result: The Custom Setup window appears and lists the Symposium Web Client components. The components that are not installed are preceded by an X.



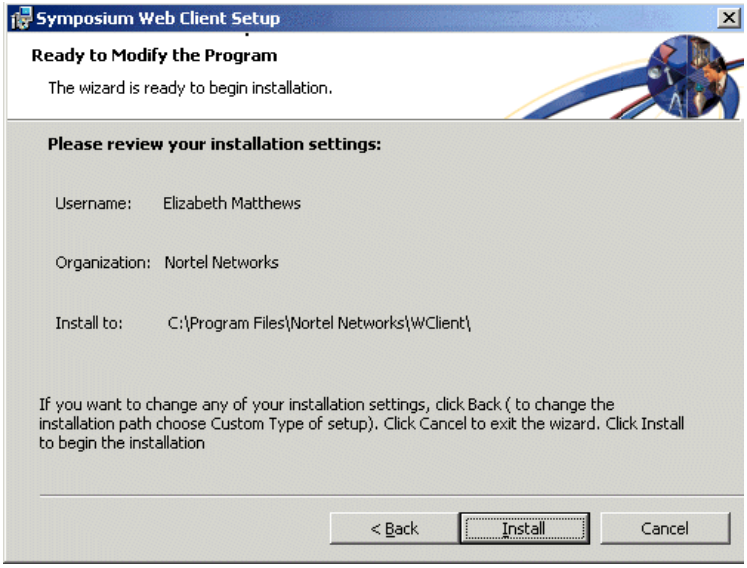
8 Click the drop-down arrow beside the name of the component that you want to add.

Note: You must install individual components from the Symposium Web Client application CD-ROM. You cannot install individual components from an upgrade *setup.exe* file.

9 On the resulting pop-up menu, click **This feature will be installed on local hard drive**.

10 Click **Next**.

Result: The Ready to Modify the Program window appears.



11 Click **Install**.

Result: The Installing Symposium Call Center Web Client window appears with a status bar that displays the progress of the installation process. When the installation is complete, the Completing Symposium Call Center Web Client Setup Wizard window appears.

12 Click **Finish**.

Result: The Symposium Call Center Web Client Installer Information window appears.

13 Click **Yes** to restart the system.

Uninstalling application server software

Introduction

This section includes separate procedures that you can perform to remove a single Symposium Web Client component, or all of the Symposium Web Client software.

ATTENTION

Before you can uninstall Symposium Web Client, you must uninstall all language packs that you have installed on the application server. To verify whether you have installed any language packs, click Start → Settings → Control Panel. Then, click **Add/Remove Programs**. All installed language packs are listed separately in the Add/Remove programs window. For more information on uninstalling them, see "To uninstall a language pack" on page 138.

Uninstalling a Symposium Web Client component

You can uninstall one or more Symposium Web Client components from the application server using the Windows 2000 Server's Add/Remove Programs feature.

To uninstall a Symposium Web Client component

1. Click Start → Settings → Control Panel.

   Result: The Control Panel window appears.

2. Double-click the **Add/Remove Programs** icon.

   Result: The Add/Remove Programs window appears.

3. Select Symposium Web Client from the list of installed programs.

4. Click **Change**.

   Result: The Symposium Web Client Setup window appears.

5. Click **Next**.

   Result: The Program Maintenance window appears.

6 Click **Modify**, and then click **Next**.

Result: The Custom Setup window appears.

7 Click the component that you want to remove, and then select **This feature will not be available** from the resulting pop-up menu.

8 Click **Next**.

Result: The Ready to Modify the Program window appears.

9 Click **Next**.

Result: The Installing Web Client window appears with a status bar that displays the progress of the uninstall process. When the uninstall is complete, the Completing Web Client Setup Wizard window appears.

10 Click **Finish**.

Result: The Web Client Installer Information window appears, indicating that you need to restart the application server for your changes to take effect.

11 Click **Yes** to restart your computer.

Uninstalling Symposium Web Client

You can uninstall the entire Symposium Web Client application by using the Windows Add/Remove Programs feature.

When you uninstall Symposium Web Client, the system prompts you to preserve user data. If you select **Yes** to preserve user data, then, during the reinstallation of Symposium Web Client, the system detects the preserved user data and prompts you to restore the data. The estimated time to complete this is 30 minutes.

To uninstall Symposium Web Client from the application server

1 Click Start → Settings → Control Panel.

2 Double-click the **Add/Remove Programs** icon.

Result: The Add/Remove Programs window appears.

3 Select Symposium Web Client from the list of installed programs.

4 Click **Change**.

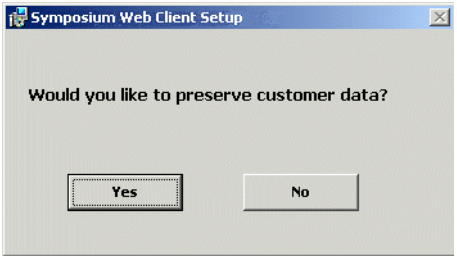
Result: The Symposium Web Client Setup window appears.

5 Click **Next**.

Result: The Program Maintenance window appears.

6 Click **Remove**, and then click **Next**.

7 The Would you like to preserve customer data? window appears.



If you want to preserve your data, click Yes. The system copies your file to the following temporary directory:

x:\Documents and Settings\Administrator\Local Settings\Temp\WClient

where x is the drive in which Windows 2000 is installed.

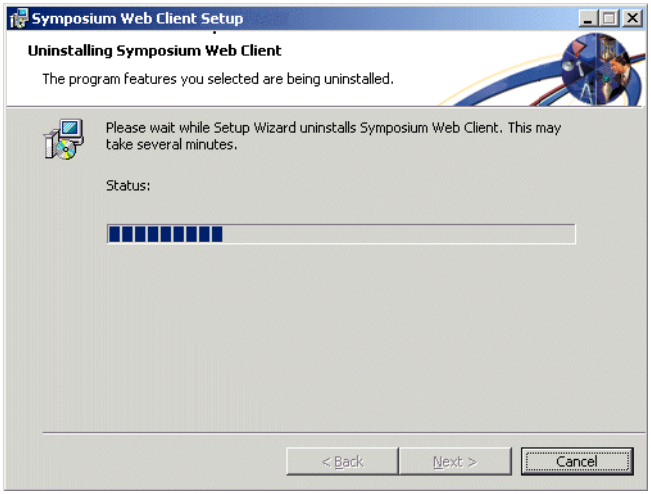
ATTENTION

If you click **No**, the system deletes all data.

Result: The Remove the Program window appears.

8 Click **Remove**.

Result: The Uninstalling Symposium Web Client window appears.



Result: The Completing the Symposium Web Client Setup Wizard window appears.

9 Click **Finish**.

Result: The Web Client Installer Information window appears, indicating that you need to restart the application server for your changes to take effect.

10 Click **Yes** to restart your computer.

Note: Uninstallation of Web Client does not automatically uninstall Active Directory.

Uninstalling Active Directory

You can uninstall Active Directory by running the Active Directory *dcpromo* program.

ATTENTION

If you are going to *reinstall* Active Directory, you must also uninstall, and then reinstall Terminal Services using Windows 2000 Server's **Add/Remove Windows Component** feature in the Add/Remove Programs window. After you reinstall Terminal Services, then reinstall Active Directory. Then you must also reconfigure Terminal Services. For more information, see "Configuring Scripting" on page 183.

Uninstall/reinstall order:

1 Uninstall Active Directory.

2 Uninstall Terminal Services.

3 Reinstall Terminal Services.

4 Reinstall Active Directory.

To uninstall Active Directory

1 Click Start → Run.

Result: The Run dialog box appears.

2 In the **Open** box, type **dcpromo**.

3 Click **OK**.

Result: The Active Directory wizard appears.

4 Follow the instructions provided by the Active Directory Installation Wizard.

Uninstalling the XML automated assignments feature

For details on uninstalling this feature, see the *XML Assignments User Guide*. This guide, and other associated documentation and engineering/development support resources for the XML automated assignments feature, are provided only through the Nortel Networks Developer Program.

For information on obtaining the XML Automated Assignment toolkit, contact a member of the Developer Program through the Contact Us link on their web site at http://www.nortelnetworks.com/developer. General information on the Developer Program, including an online membership application, is also available on this site.

Note: For overview information and details on using the XML automated assignments feature, see “Using the XML automated assignments feature” on page 426.

Configuring multiple-language support

Introduction

You can configure the Symposium Web Client application server so that you can connect to and work with a Symposium Call Center Server upon which a version of the software other than English has been installed. The steps that you must perform, however, vary according to the language in which you want to work.

In addition to English, Symposium Web Client supports the following languages:

- French
- German
- Traditional Chinese
- Japanese

The Symposium Web Client CD-ROM includes a separate language pack for each of these languages. Each language pack contains translated Historical Reporting templates, online Help, and various other files that are required for working in the language you have chosen.

Language families

Language families can be identified by their character sets. Windows uses the Latin-1 character set to display the Western European languages supported by Symposium Web Client (French and German). Therefore, these languages fall into the Latin-1 family.

Both Traditional Chinese and Japanese have distinct multi-byte character sets and, therefore, belong to individual language families (the Traditional Chinese family and the Japanese family).

English is the exception in that it is not specific to character sets; it is included in *all* language families.

For Symposium Web Client to function properly, the language family must be the same across all platforms in the network—the application server, client PCs, and Symposium Call Center Server. This means that you can mix operating systems across each of these platforms, as long as they belong to the same language family.

Example: Latin-1 languages

In your network, you can have a server in Symposium Call Center Server that has a French operating system, an application server with a German operating system, and a client PC with an English operating system. All of these languages belong to the same family (Latin-1) and, therefore, can coexist in the same network. In this case, the language preference setting on the client PC's browser determines the language in which the application is displayed.

Example: Japanese

If you want to display and enter Japanese text in Symposium Web Client, then you must install the appropriate version of the Japanese operating system on the server in Symposium Call Center Server, the application server, and each client PC. You must also configure the server in Symposium Call Center Server to handle Japanese, install the Japanese language pack on the application server, and configure the browser's language preferences for Japanese on both the application server and client PCs.

Overview of steps for configuring multiple language support

The steps that you must perform for configuring multiple language support differ according to the language in which you want to work. For information on configuring systems to display French and German, see "Steps for Latin-1 configurations (French and German)" on page 130; for Japanese, see "Steps for Japanese configurations" on page 131; and for Traditional Chinese, see "Steps for Traditional Chinese configurations" on page 132.

Note: English can be displayed on a system configured in any language family by changing the language preferences in the Internet Explorer browser.

Steps for Latin-1 configurations (French and German)

On the application server

- Ensure that the Symposium Web Client software and all required third-party software (especially Sybase Open Client v.12.5) is installed.
- Ensure that you have installed Windows 2000 Advanced Server or Windows 2000 Server with Service Pack 3 (minimum), Service Pack 4 or later (recommended) with Latin-1 language support (or the localized version of the operating system).

ATTENTION

When installing and configuring the software on the application server, you cannot install a non-English version of the operating system over a previously installed English version of the operating system. Instead, you must ensure that the application server is completely clean and free of all English operating system components before proceeding with the non-English installation. Failure to do so results in functionality problems in Symposium Web Client.

- Ensure that there are at least 225 Mbytes of free disk space before installing the language pack.
- If these conditions are met, then install the language pack of your choice (either French or German). For more information, see “To install a language pack” on page 133.
- In Internet Explorer, change the language preferences to display the language of your choice. For more information, see “To set the language preferences in Internet Explorer 5.5 Service Pack 2 (or later)” on page 139.
- Edit the locales.dat file to reflect the Latin-1 language family. For more information, see “To edit the locales.dat file” on page 141.

On the client PCs

- In Internet Explorer, change the language settings to display the language of your choice. For more information, see “To set the language preferences in Internet Explorer 5.5 Service Pack 2 (or later)” on page 139.

On Symposium Call Center Server

- Ensure that the Symposium Call Center Server Release 4.0 or 4.2 US English software is installed, along with the US English version of Windows 2000 Server (or the appropriate localized version).

Steps for Japanese configurations

On the application server

- Ensure that the Symposium Web Client software and all required third-party software (especially Sybase Open Client v.12.5) is installed.
- Ensure that you have installed the Japanese version of Windows 2000 Advanced Server or Windows 2000 Server with Service Pack 3 (minimum), Service Pack 4 or later (recommended).

ATTENTION

When installing and configuring the software on the application server, you cannot install a non-English version of the operating system over a previously installed English version of the operating system. Instead, you must ensure that the application server is completely clean and free of all English operating system components before proceeding with the non-English installation. Failure to do so results in functionality problems in Symposium Web Client.

- Ensure that there are at least 225 Mbytes of free disk space before installing the language pack.
- If these conditions are met, then install the Japanese language pack. For more information, see “To install a language pack” on page 133.
- In Internet Explorer, change the language preferences to display Japanese. For more information, see “To set the language preferences in Internet Explorer 5.5 Service Pack 2 (or later)” on page 139.
- On the application server, change the Windows regional settings to Japanese. For more information, see “To change the Windows Regional Settings” on page 140.
- Edit the locales.dat file to reflect the Japanese language family. For more information, see “To edit the locales.dat file” on page 141.

On the client PCs

- Install the Japanese version of the operating system (Windows 98/NT/2000/XP).
- In Internet Explorer, change the language settings to display Japanese. For more information, see “To set the language preferences in Internet Explorer 5.5 Service Pack 2 (or later)” on page 139.

On Symposium Call Center Server

- Ensure that the NS040206SU04S PEP (or later) and the N10402JAPANESE PEP are installed on a server running the Symposium Call Center Server Release 4.2 US English software.
- Ensure that the Japanese version of Windows 2000 Server is installed.

Steps for Traditional Chinese configurations

On the application server

- Ensure that the Symposium Web Client software and all required third-party software (especially Sybase Open Client v.12.5) is installed.
- Ensure that you have installed the Traditional Chinese version of Windows 2000 Advanced Server or Windows 2000 Server with Service Pack 3 (minimum), Service Pack 4 or later (recommended).

ATTENTION

When installing and configuring the software on the application server, you cannot install a non-English version of the operating system over a previously installed English version of the operating system. Instead, you must ensure that the application server is completely clean and free of all English operating system components before proceeding with the non-English installation. Failure to do so results in functionality problems in Symposium Web Client.

- Ensure that there are at least 225 MBytes of free disk space before installing the language pack.
- If these conditions are met, then install the Traditional Chinese language pack. For more information, see “To install a language pack” on page 133.

- In Internet Explorer, change the language preferences to display Traditional Chinese. For more information, see “To set the language preferences in Internet Explorer 5.5 Service Pack 2 (or later)” on page 139.
- On the application server, change the Windows regional settings to Traditional Chinese. For more information, see “To change the Windows Regional Settings” on page 140.
- Edit the locales.dat file to reflect the Traditional Chinese language family. For more information, see “To edit the locales.dat file” on page 141.

On the client PCs

- Install the Traditional Chinese version of the operating system (Windows 98/NT/2000/XP).
- In Internet Explorer, change the language settings to display Traditional Chinese. For more information, see “To set the language preferences in Internet Explorer 5.5 Service Pack 2 (or later)” on page 139.

On Symposium Call Center Server

- Ensure that the NS040206SU04S PEP (or later) and the N10402TCHINESE PEP are installed on a server running the Symposium Call Center Server Release 4.2 US English software.

To install a language pack

The Symposium Web Client CD-ROM includes four language packs:

- French
- German
- Japanese
- Traditional Chinese

Follow the procedure in this section to install a language pack on the application server.

Notes:

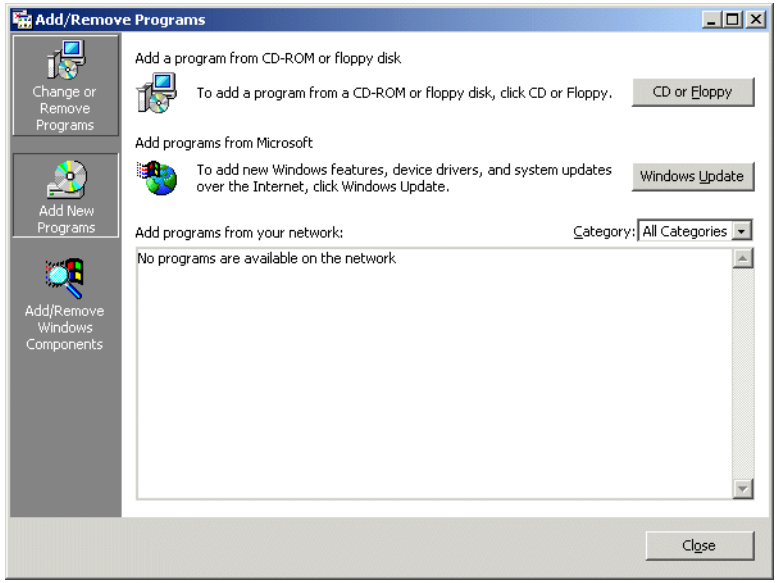
- Once you install a language pack, if you subsequently want to uninstall the Symposium Web Client software, you must uninstall the language pack

first. Then proceed with uninstalling the Symposium Web Client software. For more information, see “To uninstall a language pack” on page 138.

- To work in multiple languages in the Agent Desktop Displays component, you must perform a different series of steps. For more information, see “Configuring multiple language support in Agent Desktop Displays” on page 143.

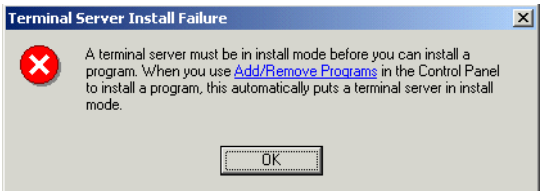
1. Click Start → Settings → Control Panel.
2. In the Control Panel window, click **Add/Remove Programs**.

   Result: The Add/Remove Programs window appears.



Note: If you double-clicked the .exe file for the language pack on the Symposium Web Client CD, the Terminal Services Install Failure dialog box

appears. This occurs because Terminal Services must be in Install Mode before you can install an application.



To switch Terminal Services to Install Mode and install the language pack, select the Add/Remove Programs link in the dialog box. The Add/Remove Programs window appears, and Terminal Services automatically switches to Install Mode.

3 Click **Add New Programs**.

4 Click CD or Floppy to indicate that you want to install the language pack from the CD-ROM.

Result: The Install Program From Floppy Disk or CD-ROM window appears.

5 Click **Next**.

Result: The Run Installation Program window appears, and D:\setup appears by default in the Open box, where D: is the CD-ROM drive.

6 Click **Browse** to navigate to the location of the language pack that you want to install. All language packs are located in the root directory of the Symposium Web Client CD-ROM, in the Language Packs folder. Navigate to this folder, and within it, double-click the folder corresponding to the language pack that you want to install.

7 In this folder, click the .exe file for language pack that you want to install. For example, to install the Japanese language pack, navigate to the Language Packs/Japanese Language Pack folder, and then click the **Japanese language pack.exe** file.

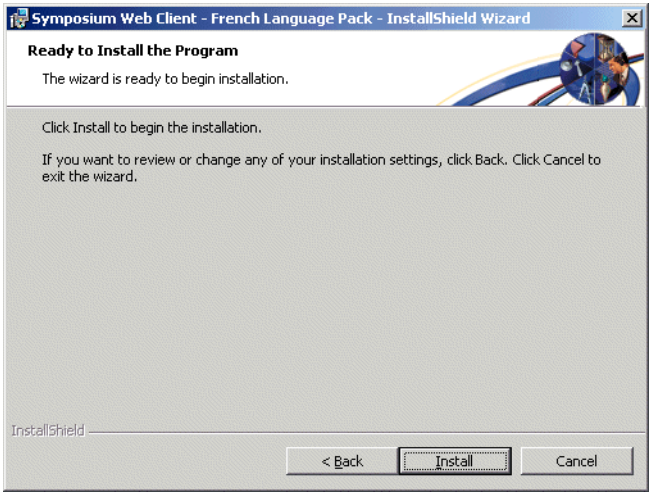
Result: The path to the correct language pack .exe file appears in the Open box.

8 Click **Finish**.

Result: The InstallShield Wizard window appears briefly, followed by the Windows Installer window. When the installer finishes its prerequisite check, the welcome window appears.

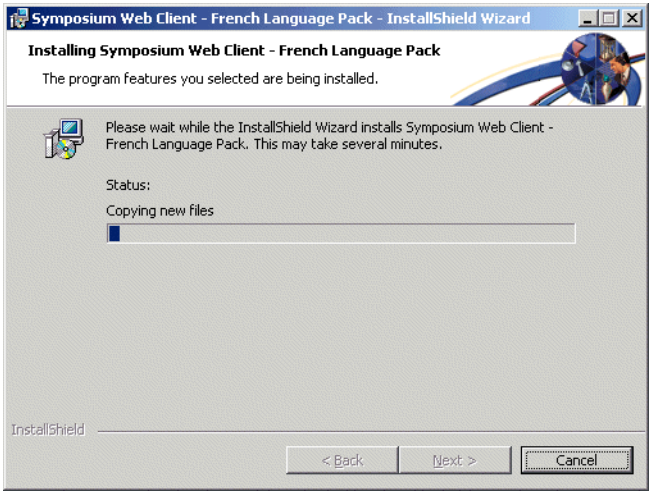
9 Click **Next**.

Result: The Ready to Install the Program window appears.

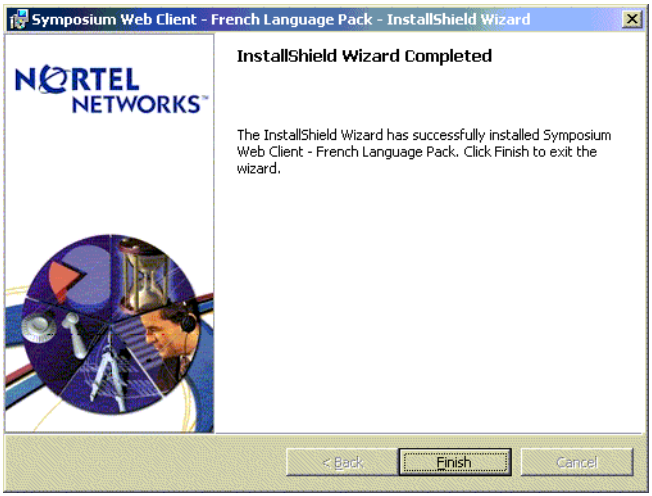


10 Click **Install**.

Result: The Installing Symposium Web Client - *X* Language Pack window appears (where *X* is the language you have chosen).



11 The program copies and installs the required files. When it is finished, the InstallShield Window Completed window appears.



12 Click **Finish**.

Tip: You can view the language packs that you have installed on the server by clicking Start → Settings → Control Panel. Then click **Add/Remove Programs**. The Add/Remove Programs window lists the language packs installed on the server and their version numbers.

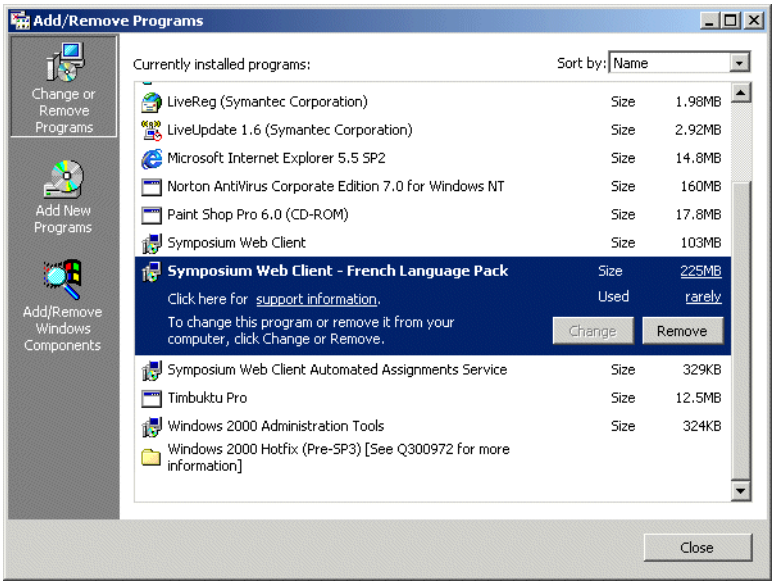
To uninstall a language pack

Note: Once you install a language pack, if you subsequently want to uninstall the Symposium Web Client software, you must uninstall the language pack *first*. Then proceed with uninstalling the Symposium Web Client software.

1 Click Start → Settings → Control Panel.

2 In the Control Panel window, click **Add/Remove Programs**.

3 In the Add/Remove Programs window, highlight the language pack that you want to uninstall.



4 Click **Remove**.

5 The program asks you to confirm your choice. Click **Yes**.

6 The program removes the language pack from the application server.

To set the language preferences in Internet Explorer 5.5 Service Pack 2 (or later)

You must perform this procedure on each client PC that will be connecting to the application server to use Symposium Web Client. Perform this procedure on the application server only if you will also be using it as a client PC.

Note: In addition to these steps, you must also set the proper security level settings in the browser. For more information, see "To configure Internet Explorer 5.5 Service Pack 2 (or later)" on page 294, or "To configure Internet Explorer 6.0 Service Pack 1 (or later)" on page 297.

1 In Internet Explorer, click Tools → Internet Options.

Result: The Internet Options window appears.

2 Click **Languages**.

Result: The Language Preferences window appears.

3 Verify that the language you want to use appears in the Language box. The codes for the languages supported by Symposium Web Client are as follows:

- English [United States] [en-us]
- French [France] [fr]
- German [Germany] [de]
- Chinese [Taiwan] [zh-tw]
- Japanese [ja]

4 If the language does not appear in the box, then you must add it as follows:

a. Click **Add**.

Result: The Add Language window appears.

b. From the list of languages, click the appropriate language, and then click **OK**.

Result: The language now appears in the Language Preferences window.

c. Proceed with the next step to move the language to the top of the box.

5 If the language you want to use appears in the box, then you must move it to the top of the list as follows:

a. In the Language box, click the appropriate language.

b. Click **Move Up** until the language appears at the top of the box.

c. Click **OK** to close the Language Preferences window.

6 Click **OK** to close the Internet Options window.

To change the Windows Regional Settings

You must change the Regional Settings on the application server if you are using either the Japanese or Traditional Chinese versions of Symposium Web Client. It is not necessary to perform this procedure if you are using the English, French, or German versions of the software because all of these languages display properly with the Regional Settings set to the default language, English.

1 On the application server, click Start → Settings → Control Panel.

2 Double-click the Regional Options icon.

Result: The Regional Options window appears.

3 From the Your locale drop-down list on the General tab, choose the appropriate locale:

- for Traditional Chinese, choose **Chinese** (Taiwan)
- for Japanese, choose **Japanese**

4 In the Language settings for the system box, click the check box beside the appropriate language (either Traditional Chinese or Japanese).

5 Click **Set default**.

Result: The system asks if you want to install additional language files from your operating system CD.

6 Insert your operating system CD into the server, and then click **OK**.

7 When the system has finished installing the files, click **OK** to save your changes and close the Regional Options window.

8 Close the Add/Remove Programs window.

To edit the locales.dat file

To edit the locales.dat file, you can use the utility that comes with Symposium Web Client and is stored on the application server. You can access this utility from any client PC (or from the application server, when used as a client PC) by first logging on to Symposium Web Client, and then opening the utility through the browser window. The utility enables you to configure the system to handle the character set of the language family with which you want Symposium Web Client to work.

1 From any client PC (or the application server when used as a client PC), open Internet Explorer and log on to Symposium Web Client.

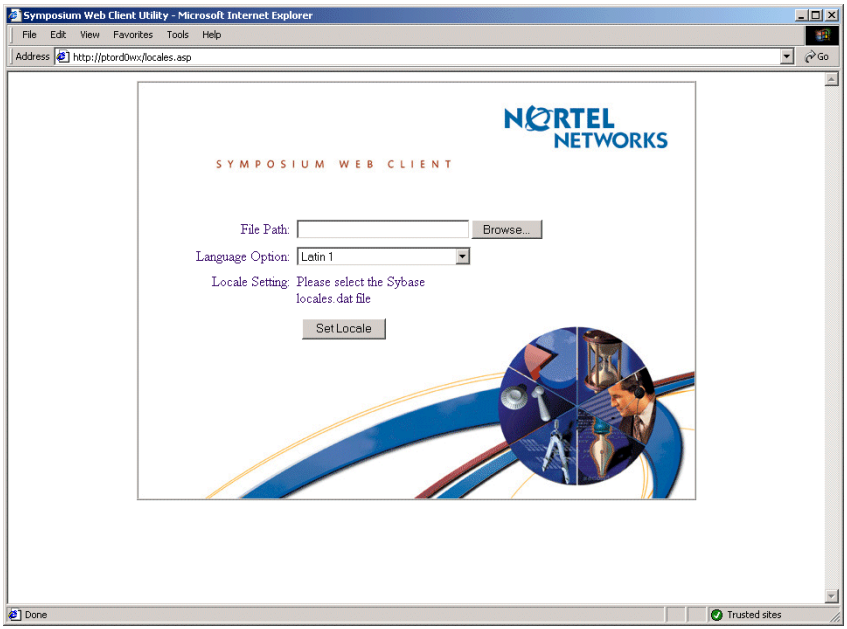
2 In the browser's address box, type the following:

http://*localhost*/locales.asp

where *localhost* is the name or IP address of the application server.

3 Press **Enter**.

Result: The utility opens.



4 Click **Browse** to navigate to the ***c:/sybase/locales/locales.dat*** file, where *c:* is the drive on which you installed Sybase Open Client v.12.5.

5 From the **Language Option** drop-down list, select the appropriate language. You can choose from Latin 1, Japanese, and Traditional Chinese.

6 Click **Set Locale** to save your changes.

7 You can now continue working in Symposium Web Client.

Configuring multiple language support in Agent Desktop Displays

Introduction

To work in multiple languages in Agent Desktop Displays (ADD), you must first install the ADD server software containing the translated language components on the application server. This version of the software is available on the Symposium Web Client 4.5 CD-ROM as part of the general Symposium Web Client software installation.

Then, you must install the client portion of the ADD software on each client PC that will be used to launch Agent Desktop Displays. For more information on installing the client software, see “Installing and configuring Agent Desktop Displays on a client PC” on page 322.

To change the language in which you view the displays, log on to Agent Desktop Displays, and then right-click on the display. A series of languages appears in a menu, enabling you to choose the language in which you want to work. The languages available are only those for which there are localized strings installed. These languages must also belong to the same language family in which Agent Desktop Displays is installed.

Note: If you already have the correct version of the ADD client software installed on the client PCs, when you install the software on the application server, it automatically upgrades the ADD client installation with the translated text. If you do not have ADD installed on the client PC, then you must manually install the ADD software with the language pack content on each client PC. Consult the table below for the ADD client versions supported by the automatic multi-language support upgrade.

Versions of ADD client software and multiple language support

Note: If the client operating system is Windows NT 4.0 Workstation, Windows XP, or Windows 2000, you need Administrator privileges to install Agent Desktop Displays. You do not need administrator privileges if the client PC runs Windows 98.

Version of ADD software installed on client PC	Steps to configure multiple language support on client PC
Earlier version than build 04.02.011.00 (SU08).	On the application server, install ADD with multi-language support from the Symposium Web Client CD-ROM version 04.02.016.04 (or later). This installation automatically upgrades the software on each client PC with the translated versions of ADD for all languages supported.
No ADD software is installed.	If there is no ADD software installed on the client PCs, then, after you install the Symposium Web Client software on the application server, you only have to install the client ADD software by following the normal installation instructions. For more information, see “Installing and configuring Agent Desktop Displays on a client PC” on page 322.

Section D: Backing up and restoring user data

In this section

Overview	146
Backing up Symposium Web Client data	148
Restoring Symposium Web Client data	153
Replication considerations	161

Overview

Introduction

You can help your call center to recover from events, such as data loss and damage due to disk failures and power outages, by creating a backup of your call center data. This applies to both to data on the Symposium Web Client application server and on the server in Symposium Call Center Server.

When to back up Symposium Web Client data

Nortel Networks recommends that you back up your call center data at least once a day (or more frequently, based on your call center requirements).

At minimum, to ensure that Symposium Web Client data and Symposium Call Center Server data is synchronized, and to ensure the proper functionality of Symposium Web Client, it is imperative that *each time* you back up the Symposium Call Center Server database, you must perform a backup of the application server *at the same time*. Likewise, you must restore the Symposium Web Client application server and the Symposium Call Center Server database *at the same time*. However, note that you can back up the application server on its own as often as required, without needing to back up Symposium Call Center Server at the same time.

Note: You can schedule Symposium Web Client backups to run on an ongoing basis using the Windows backup tools.

Why you need to back up data

Backups can help you in the following scenarios:

- When you upgrade to newer versions of Symposium Web Client, perform a backup just before upgrading so you can revert back to the previous version of the software, if necessary.
- You can use backups when you want to roll back erroneous data.

- You can use data backups of your application server to help your call center to recover from catastrophic events (such as data loss and damage due to disk failures and power outages).

Which data is backed up

When planning your backup strategy, it is useful to know which data is stored on the Symposium Web Client application server and which data is stored on the server in Symposium Call Center Server.

- Symposium Call Center Server data includes
  - agents, supervisors, skillsets and all their related assignments (accessed through Contact Center Management)
  - CDNs, DNISs and all the other data items (accessed through the Configuration component)
- Symposium Web Client data includes
  - schedule information for historical reports
  - partitions, access classes, report groups, and the Web Client users
  - real-time display configuration data and real-time display filters
  - private historical reports
  - Contact Center Management scheduled assignment information

Backing up Symposium Web Client data

Introduction

Symposium Web Client makes use of Active Directory and other data files to store user data. Therefore, you need to back up both Active Directory and the data files listed below.

In addition, during the backup, you must ensure that no data is changed between backing up Active Directory and the data files. It is recommended, therefore, that you perform backups during periods of low activity.

Backing up Symposium Web Client Active Directory data

Symposium Web Client stores Access and Partition Management data and some Historical Reporting and Real-Time Reporting data in Active Directory. You must back up this data regularly.

To back up this data, Microsoft provides a Windows 2000 backup utility called Microsoft Windows Backup Tool. This tool performs the Active Directory backup as part of the System State data backup. In addition to Active Directory data, System State data includes interdependent items, such as the registry, system startup files, the class registration database, certificate services database, file replication service, cluster service, and the domain name service.

You have two options when performing an Active Directory backup:

- **Microsoft Windows Backup Wizard** To perform an Active Directory backup using the Microsoft Windows Backup Wizard, follow the five steps listed in “To back up System State data using the Backup Wizard,” which can be found in Microsoft’s “Backing Up Active Directory” procedure in the Windows 2000 Server documentation. As of the date of publication of this guide, you can find this documentation at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/reskit/distsys/part1/dsgch09.asp.
- **Microsoft Windows Backup Tool graphical user interface** You can also back up Active Directory by using the Microsoft Windows Backup Tool graphical user interface. To do so, follow the five steps listed in “To back up

System State data manually by using the GUI," which can be found in Microsoft's "Backing Up Active Directory" procedure in the Windows 2000 Server documentation. As of the date of publication of this guide, you can find this documentation at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/reskit/distsys/part1/dsgch09.asp.

You may also want to consult the Microsoft documentation for other backup strategies. One important point to consider when choosing a backup utility is that it must allow you to back up both System State data (which includes Active Directory data and registry information) and other files stored in the operating system. If you want to be able to schedule backups, then you must ensure that your backup tool enables you to back up all these types of files without requiring you to manually copy any of them. Choose the strategy that is most appropriate for your organization.

Note: Nortel Networks has also tested the Veritas Backup Exec 9.0 tool, which can be used instead of the Microsoft Windows Backup Tool to back up Active Directory data. There are several other third-party tools that can perform a similar function; choose the tool that best suits your organization.

Backing up Symposium Web Client data files

In addition to storing user data in Active Directory, Symposium Web Client stores other user information in various data files, which also must be backed up. The types of files that you must back up include the following:

- historical report data
- real-time display snapshots
- Emergency Help snapshots
- schedule data

There are two options for backing up these files:

- **Manually copying files** The first option is to manually copy the files to a secure storage location, such as a tape drive or a safe network drive.
- **Windows Backup Tool** The second option is to use the Windows Backup Tool to back up the Symposium Web Client data files and the System State data. However, you can only use this method when the version of

Symposium Web Client to which you are restoring data is the same as the version of Symposium Web Client from which you backed up the data.

Manually copying files

Copy the files listed below to a secure storage location (for example, a tape drive or a safe network drive).

In the following default path,

C:\Program Files\Nortel Networks\WClient\Apps\Reporting\Historical\data

where C: is the drive on which Symposium Web Client is installed, back up these files:

- LimitChecker.mdb
- Netcallbycall.mdb
- nicrpt.mdb
- nicrpt_dms.mdb
- schedule.mdb (this file contains Historical Reporting schedule information)
- custform.mdb

In the following default path,

C:\Program Files\Nortel Networks\WClient\Apps\Common\Icedb

where C: is the drive on which Symposium Web Client is installed, back up these files:

- Schedule.mdb (this file contains Contact Center Management schedule information)
- icelog.mdb

In the following default path,

C:\Program Files\Nortel Networks\WClient\Apps\AccessMgmt\AccessXML

where C: is the drive on which Symposium Web Client is installed, back up this file:

- counter.xml

In addition to the files listed above, you must also back up any files that you have saved on the application server for Symposium Web Client operations, such as custom report templates, Historical Reporting output files, or snapshots of real-time displays and emergency help panels. The locations of these files are decided by the user. The default paths are listed below:

- Real-time display snapshots are stored as HTML files in the following default path,

  C:*Program Files\Nortel Networks\WClient\Apps\Reporting\Real-time\Exports*

  where C: is the drive on which Symposium Web Client is installed.
- Emergency Help snapshots are stored as HTML files in the following default path,

  C:*Program Files\Nortel Networks\WClient\Apps\EmergencyHelp\Exports*

  where C: is the drive on which Symposium Web Client is installed.

Backing up data using the Windows Backup Tool

You can back up the Symposium Web Client data files, as well as the Symposium Web Client Active Directory data using the Windows Backup Tool. To do so, you must back up the Symposium Web Client files listed in the preceding section, in addition to the System State data.

Note: You can only use this method when the version of Symposium Web Client to which you are restoring data is the same as the version of Symposium Web Client from which you backed up the data.

To use this method, follow the procedure "To back up System State data manually by using the GUI," which is listed within Microsoft's "Backing Up Active Directory" documentation. As of the date of publication, you can find this documentation at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/reskit/distsys/part1/dsgch09.asp.

When following this procedure, in step 2 you must also select the following directories:

- *C:\Program Files\Nortel Networks\WClient\Apps*

  where C: is the drive on which Symposium Web Client is installed

- the directories where you have stored the following types of files (if not under the folder specified in the previous bullet):
  - historical report output files
  - custom report templates
  - real-time display snapshots
  - Emergency Help snapshots

Notes:

- Real-time display snapshots are stored as HTML files in the following default path:

  C:\Program Files\Nortel Networks\WClient\Apps\Reporting\Real-time\Exports

  where C: is the drive on which you installed Symposium Web Client
- Emergency Help snapshots are stored as HTML files in the following default path:

  C:\Program Files\Nortel Networks\WClient\Apps\EmergencyHelp\Exports

  where C: is the drive on which you installed Symposium Web Client

Scheduling backups

The Windows Backup Tool has a scheduling component that you can use to schedule automatic backups of data, possibly to run at night when the call center is quiet, or to synchronize Symposium Web Client backups with scheduled Symposium Call Center Server backups.

To schedule a backup, follow the procedure outlined above in the section “Backing up data using the Windows Backup Tool” on page 151. After specifying the folders required, go to the “Schedule jobs” section of the Windows Backup Tool utility.

Restoring Symposium Web Client data

Introduction

There are several scenarios where it is necessary to restore Symposium Web Client data, including

- recovery from a Symposium Web Client application server hardware failure
- when Symposium Call Center Server data is being restored
- if you are reverting the Symposium Web Client software back to a previous version
- if you made an error while entering Symposium Web Client data and you need a previous version of the data. (Symposium Web Client data is all data excluding configuration data, scripts, and agents and supervisors.)

Notes:

- You must ensure that Active Directory and the data files that you are restoring were backed up at the same time; that is, you must ensure that the Symposium Web Client data did not change between backing up Active Directory and the user data files. Nortel Networks recommends that you perform backups during periods of low activity.
- You cannot use the application server while restoring data.
- You can use the Windows Backup Tool or a similar tool to restore the System State data. However, the tool you use must be capable of restoring both the Active Directory data (which is included in the System State data), and, if scheduled backups are used, the Symposium Web Client data files that you backed up. The procedure in this section is based on the Windows Backup Tool method of restoring data.
- You cannot restore a backup image that is older than the *tombstone lifetime* setting because your backup image may contain objects that have already been deleted and cannot be recovered. The *tombstone lifetime* is the number of days that a deleted object is maintained before the garbage collection process permanently removes it from Active Directory. The default value is 60 days. For more information, see the article “Backup of the Active Directory Has 60-Day Useful Life (Q216993)” on the Microsoft web site.

Recovery from a Symposium Web Client application server hardware failure

If the Symposium Web Client application server hardware fails, it may be necessary to restore the data to another server.

When restoring data onto a different application server, since you restore the System State data (which includes registry information) from the “source” server, your “target” server inherits attributes, such as the computer name and IP address, and any software that was installed on the source server. This information also resides in the registry.

You must ensure that the location of the system root on the target application server is the same as that on the source application server.

To restore Active Directory onto a target application server that has a different hardware platform, first note the following:

- The target server must have the same type of hard disk controllers as the source server; that is, it must have either Small Computer System Interface (SCSI) or Integrated Drive Electronics (IDE).
- The size of the target server hard disk must be at least as large as that of the source server.
- If your target server has a different video adapter or multiple network adapters, then you must uninstall them before you restart the server. The normal Plug-and-Play functionality makes the appropriate updates once you restart the server.
- To simplify the restore procedure, Nortel Networks recommends that both the source and target application servers support the same number of processors.
- As a precaution, install on the target server any software that was installed on the source server. Even though the registry holds all software that was installed on the source server, by installing the same software, you reduce the chance of problems occurring when you complete the restore.

Restoring Symposium Web Client data onto a new application server

This section outlines the steps you need to perform to back up Symposium Web Client data from one application server and restore the same data to a brand new application server. You can use this procedure to recover from a system failure should your Symposium Web Client application server fail completely (for example, due to hardware problems).

1. Use the backup that you have already created. For more information on creating backups, see “Backing up Symposium Web Client data” on page 148.

Note: Nortel Networks recommends that perform backups as often as necessary to always have copies of the latest data.

2. Follow the installation instructions listed in the installation checklists to install and configure the Windows 2000 Server operating system, all third-party software (such as Microsoft Active Directory and Sybase Open Client), pcAnywhere (if it is installed on the original application server), and Symposium Web Client on your new application server. For details, see Appendix A, “Installation worksheets and checklists.”

Note: Nortel Networks recommends that you install all software in the same directories as those used on your original application server.

3. When the server is restarted, restore the data from the backup taken earlier. To do this, follow the procedure “Using the Backup Tool to Restore Active Directory” specified in the “Restoring Active Directory from Backup Media” section of the Microsoft Windows 2000 Server documentation. As of the date of publication, you can find this documentation at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/reskit/distsys/part1/dsgch09.asp.

Notes:

- Before you can restore the System State data, you must restart the server in Directory Services Restore Mode. To do so, while the server is starting up, press **F8**, and then select the Directory Services Restore Mode option.
- When using the Windows Backup Tool to restore the Symposium Web Client data files, it is very important that you select the option to always replace the files on the computer. As of the time of writing, you can select this option in the **Restore** tab of the Options window (accessible from the

Tools menu), or when you are using the Restore Wizard in the Advanced Options "How To Restore" page.

- If the application server is the sole domain controller in the domain, an authoritative restore is not required. However, if the application server is running in a replication environment, and is not the sole domain controller in the domain, an authoritative restore may be required. For more information on authoritative restoration, see http://support.microsoft.com/default.aspx?scid=kb;en-us;216243.

4. If you did not include the Symposium Web Client data files in the backup used in step 3, then restore the Symposium Web Client data files to their original paths. See “Restoring Symposium Web Client data files” on page 157 for more information. You must perform this step before proceeding to the next step.

5. Using Symposium Web Client, reactivate any scheduled historical reports and Contact Center Management assignments. To do so, you may need to deactivate the scheduled historical reports first.

After completing this final step, you can now use Symposium Web Client on your new application server. Since this new server has the same computer name and IP address as the original server, ensure that the two servers are not active on the same network at the same time.

Note: You may have third-party software applications other than those mentioned in step 2 installed on your original application server. Nortel Networks recommends that you install the same applications on your new application server. For example, if pcAnywhere was installed on the source application server, then you must install pcAnywhere on the target application server. For a complete list of software requirements on the application server, see “Application server software requirements” on page 27.

For more details consult the Microsoft documentation at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/ad/windows2000/support/adrecov.asp.

Restoring Symposium Web Client data files

If the backup file you used to restore the System State data did not contain the Symposium Web Client data files, then you must copy these data files to the server manually.When restoring data files, ensure that you restore all the backed up files to their original paths, as listed in the previous section on backing up data.

Restore these files

- LimitChecker.mdb
- Netcallbycall.mdb
- nicrpt.mdb
- nicrpt_dms.mdb
- schedule.mdb
- custform.mdb

to the following path, where C: is the drive on which you installed Symposium Web Client:

C:\Program Files\Nortel Networks\WClient\Apps\Reporting\Historical\data

Restore these files

- Schedule.mdb
- icelog.mdb

to the following path, where C: is the drive on which you installed Symposium Web Client:

C:\Program Files\Nortel Networks\WClient\Apps\Common\Icedb

Restore this file

- counter.xml

to the following path, where C: is the drive on which you installed Symposium Web Client:

C:\Program Files\Nortel Networks\WClient\Apps\AccessMgmt\AccessXML

In addition to the files listed above, you must also restore any files that you have saved on the application server for Symposium Web Client operations, such as custom report templates, Historical Reporting output files, or snapshots of real-time displays and Emergency Help panels. The locations of these files are decided by the user. The default paths are listed below:

- Real-time display snapshots are stored as HTML files in the following default path, where C: is the drive on which you installed Symposium Web Client:

  C:\Program Files\Nortel Networks\WClient\Apps\Reporting\Real-time\Exports

- Emergency Help snapshots are stored as HTML files in the following default path, where C: is the drive on which you installed Symposium Web Client:

  C:\Program Files\Nortel Networks\WClient\Apps\EmergencyHelp\Exports

Restoring Symposium Web Client data onto the same application server

Perform the following steps to restore Symposium Web Client data onto the same server from which it was backed up:

1. Using the backup of data that you have taken, follow the procedure “Using the Backup Tool to Restore Active Directory” specified in the “Restoring Active Directory from Backup Media” section of the Microsoft Windows 2000 Server documentation. As of the date of publication, you can find this documentation at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/reskit/distsys/part1/dsgch09.asp.

Note: If the application server is the sole domain controller in the domain, an authoritative restore is not required. However, if the application server is running in a replication environment, and is not the sole domain controller in the domain, an authoritative restore may be required. For more information on authoritative restoration, see http://support.microsoft.com/default.aspx?scid=kb;en-us;216243.

2. If you did not include the Symposium Web Client data files in the backup used in step 1, then restore the Symposium Web Client data files to their

original paths. See “Restoring Symposium Web Client data files” on page 157 for more details.

3. Delete any scheduled tasks (scheduled historical reports and Contact Center Management assignments) that are no longer required from the Windows Task Scheduler. You can open the Scheduler in Windows 2000 by clicking Start → Programs → Accessories → System Tools → Scheduled Tasks.

4. Use Symposium Web Client to reactivate any scheduled tasks that you have restored and require (historical reports and Contact Center Management assignments).

Restoring Symposium Call Center Server data

To prevent synchronization issues, you must restore the Symposium Web Client data whenever you restore the Symposium Call Center Server data. To restore the Symposium Web Client data, follow the procedure outlined in “Restoring Symposium Web Client data onto the same application server” on page 158. Also, you must ensure that the Symposium Web Client data was backed up at the same time when the Symposium Call Center Server data was backed up.

Since Symposium Call Center Server backups may be scheduled to occur automatically when the call center is not busy, and possibly when an administrator is not available, you must ensure that you also schedule Symposium Web Client backups to occur at the same time as these backups. For information on scheduling a Symposium Web Client backup, see “Scheduling backups” on page 152.

Note: Since the backups must occur at the same time, you must ensure that the time of the servers in question is synchronized when scheduling a backup.

Reverting back to a previous version of Symposium Web Client

When reverting back to a previous version of Symposium Web Client, you must restore the Symposium Web Client data that you backed up just before upgrading. This is necessary because different versions of Symposium Web Client may access different structures in Active Directory. See “To revert back to a previous version” below for details.

Note: To restore the Symposium Web Client data, follow the procedure outlined in “Restoring Symposium Web Client data onto the same application server” on page 158.

To revert back to a previous version

When reverting back to a previous version of Symposium Web Client, follow these general steps:

1. Make a complete backup of the server (in the event that you want to perform an upgrade).
2. Uninstall the current version of the Symposium Web Client software, including the Agent Desktop Displays client software.
3. Uninstall Sybase 12.5. For information on uninstalling the software, see the documentation posted on the Sybase web site at http://manuals.sybase.com/onlinebooks/group-as/asp1200e/aseinsnt.
4. Reinstall Sybase 12.0.
5. Install the version of Symposium Web Client and Agent Desktop Displays client software to which you want to revert, choosing not to preserve customer data.
6. Restore Active Directory and other user data from the same version of Symposium Web Client to which you are reverting. For more information, see “Restoring Symposium Web Client data onto the same application server” on page 158. While restoring, perform the following steps:
   - **a.** Restart the application server in Directory Services Restore Mode by pressing **F8** when the server is starting up.
   - **b.** Restore the system state data using the backup and restore utility of your choice.
   - **c.** Restart the server in normal mode.
   - **d.** Restore the data files listed in “Restoring Symposium Web Client data files” on page 157.

Replication considerations

Introduction

You cannot use replication as your only backup and restore mechanism since you may need to revert the Symposium Web Client data to synchronise it with a Symposium Call Center Server restoration, or revert to previous versions of Symposium Web Client.

You can, however, use replication to help migrate the Symposium Web Client Active Directory data and the structure of the application server from one hardware platform to another. This has an advantage over restoring the System State data in that you do not need to reload hardware drivers (for example, the drivers required for different network interface cards), when the hardware platforms are different.

To migrate the Symposium Web Client Active Directory data from one application server to another, see “Restoring Active Directory Through Reinstallation and Replication” within the procedure “Backing Up Active Directory” in the Microsoft Windows 2000 Server documentation. As of the date of publication, you can find this documentation at http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/windows2000/techinfo/reskit/en-us/distrib/dsbh_rep_jfbg.asp.

Once you have replicated the Active Directory data, you must copy the Symposium Web Client data files to the new server. See “Restoring Symposium Web Client data files” on page 157 for details on the files to copy. Finally, you must activate any scheduled historical reports and Contact Center Management assignments.

Note: The versions of Symposium Web Client running on each of the servers must be the same.

With replication, the same Symposium Web Client users can access the same access classes, partitions, historical report groups and real-time reports on different Symposium Web Client application servers.

It is important to note, however, that scheduled data (for example, scheduled assignments and scheduled historical reports) is not replicated and is, therefore, only available to users accessing the same Symposium Web Client application server. This is also true of report outputs stored locally on an application server.

Section E: Configuring the application server

In this section

Overview	164
Configuring Real-Time Reporting	165
Configuring Emergency Help	173
Configuring Historical Reporting	175
Configuring Scripting	183
Configuring Agent Desktop Displays	194

Overview

Introduction

Before you can use Symposium Web Client, you must configure the components you have installed on the application server. The following table provides a high-level overview of items that you must configure:

For the following component	you must configure
Real-Time Reporting	the sending and receiving IP multicast addresses on the application server.
Agent Desktop Displays	the Configuration Parameters window on the application server.
Historical Reporting	SMTP, printers, and file export folders.
Scripting	the Terminal Services user in Active Directory, access rights to the Scripting component, Terminal Services, and the printer.
Emergency Help	the sending IP multicast address that the application server uses to send Emergency Help messages to client PCs.

Configuring Real-Time Reporting

Introduction

For Web Client's Real-Time Reporting component to function properly, you must configure two different IP multicast addresses:

- the application server's *receiving* IP multicast address (the address it uses to *receive* multicast data from Symposium Call Center Server; it is the same as the *sending* IP multicast address on Symposium Call Center Server)
- the application server's *sending* IP multicast address (the address it uses to *send* multicast data)

Note: The application server's sending and receiving IP multicast addresses must be different.

The application server constantly monitors its receiving IP multicast address and directs data as soon as it is available to its sending IP multicast address.

Note: The IP multicast *sending* address must be configured on Symposium Call Center Server.

Multicast compared to unicast data transmission

After you have configured the multicast addresses, you can choose the method by which you want to receive real-time data on the client PCs: multicast, unicast, or a combination of both multicast and unicast. Then, when a user launches the real-time displays, and while the system is retrieving data, an icon appears on the display, identifying whether the application server supports multicast clients, unicast clients, or both multicast and unicast clients. For more information on these icons, see "Multicast and unicast icons in real-time displays" on page 521.

Note: The unicast communication option applies *only* between the application server and the client PCs. Since the application server receives all the raw data from each server in Symposium Call Center Server through multicast channels, this network segment must always be multicast-enabled.

In certain circumstances, not all segments of a network are multicast-enabled (for example, when the network equipment cannot support multicast, or when the client PCs are at remote locations and connect over WAN or dialup links that do not support multicast). The unicast option can be used to provide users located in the non-multicast sections with real-time data.

Note: If you choose, at a later date, to multicast-enable your entire network, you may do so without having to upgrade Symposium Web Client.

Multicast data transmission

This form of data transmission provides multipoint communication by simultaneously delivering information from one sender (the application server) to multiple receivers (client PCs) who want to receive the information. The greatest advantage of IP multicasting is its ability to transmit information to many recipients in a way that minimizes both the bandwidth required to communicate across networks, and the resources required by the sender to carry out the transmission.

This type of data transmission enables users to view nodal real-time displays, network-consolidated real-time displays, Agent Desktop Displays, and Emergency Help notifications on the client PCs.

Unicast data transmission

Unicast data transmission requires that each client receive its own copy of the data; therefore, a unicast configuration uses more network bandwidth than a multicast configuration. In unicast, the data packets are duplicated on the network, whereas in a multicast environment, each packet is sent only once.

Real-time displays viewed on one client PC that use the same data stream share a single connection to the application server (for example, a standard agent display and a private agent display both use the agent moving window stream and can share a single unicast connection). Therefore, for *n* client displays of different statistical types, there are *n* separate data streams in operation, which introduces additional traffic on the network.

If a client opens a collection display (six displays in one screen), several unicast channels are opened from the application server to the client computer, one for each statistic type in the collection.

Unicast data transmission enables users to view

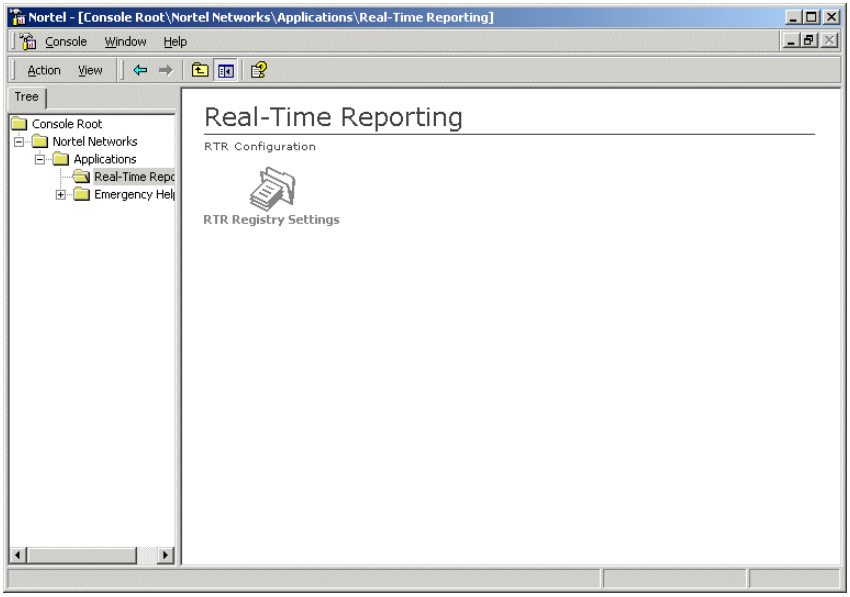
- nodal real-time displays *only* if there is an application server located at each Symposium Call Center Server node in the network
- both nodal and network-consolidated real-time displays if the network between the application server and *each* server in Symposium Call Center Server is multicast enabled

Agent Desktop Displays and Emergency Help notifications are not available on client PCs that only receive unicast data.

To configure Real-Time Reporting

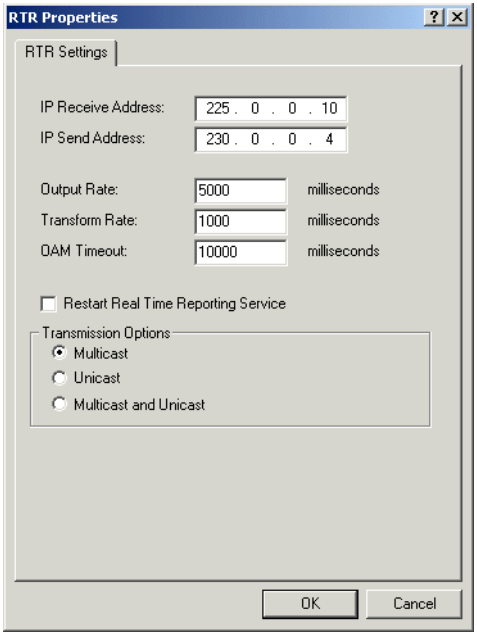
1 Click Start → Programs → Symposium Web Client → Configuration.

Result: The Real-Time Reporting window appears.



2 Click the **RTR Registry Settings** icon in the right pane of the console window.

Result: The RTR Properties window appears.



3 In the **IP Receive Address** and **IP Send Address** boxes, type the correct address information. The IP Receive address in Symposium Web Client must be the *same* as the IP send address in Symposium Call Center Server; however, it must be *different* from the IP Send address in Symposium Web Client.

ATTENTION

If the server in Symposium Call Center Server is part of a networked call center, all servers in Symposium Call Center Server within the network must have the same IP Send address. The IP Receive address for Symposium Web Client must match the common IP Send addresses of the servers in Symposium Call Center Server.

4 Accept the default values in the **Output Rate** box (5000) and the **Transform Rate** box (1000). You can adjust the default values; however,

reducing the Output Rate value and the Transform Rate value increases the workload on the application server.

Note: The fastest rate at which multicast data from Symposium Call Center Server reaches the end user in Symposium Web Client is equal to the highest value among the following settings:

- the Multicast Rate at which data is sent from Symposium Call Center Server to the Symposium Web Client application server (For more information on Multicast Rates, see “Modifying RSM settings and multicast rates” on page 51.)
- the Output Rate at which the application server outputs data to client PCs
- the Transform Rate at which the application server processes data

Example
If the Symposium Call Center Server Multicast Rate is set to 2 seconds, the application server Transform Rate is set to 1 second and the application server Output Rate is 7 seconds, then the data on the client PC will not refresh faster than every 7 seconds, regardless of the refresh rate that the user has chosen in Real-Time Reporting.

If you want to decrease the length of time required for real-time statistics to reach client PCs, you can decrease the Output Rate and Transform Rate values; however, this impacts performance on the application server. You should notify users of the Real-Time Reporting component of these rates so they can adjust the refresh rate accordingly. For more information on adjusting rates and assessing performance, see the Capacity Assessment Tool (CapTool) chapter of the *Symposium Call Center Server Planning and Engineering Guide*.

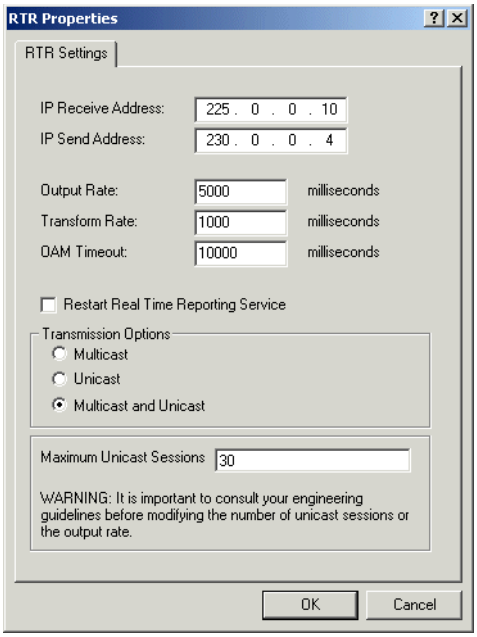
5 Accept the default value in the **OAM Timeout** box (10 000).

ATTENTION

You may have to increase this value if the following occurs:
When creating or viewing a partition in Access and Partition Management, you cannot see any partition elements in the right pane. This can occur when there is a large amount of data stored on Symposium Call Center Server and the network is slow. If you increase the OAM Timeout value, it provides more time for the partition elements to be collected on a per-server basis. It is recommended that you increase this value in increments of 10 000 (milliseconds).

6 In the Transmission Options area, click the radio button beside the transmission mode that is required for the site. Choose **Multicast** only if your network supports multicast traffic (recommended), **Unicast** only if you do not want any multicast traffic on your network, or **Multicast and Unicast** if you want to support both transmission types.

7 If you select either **Unicast** or **Multicast and Unicast**, the Maximum Unicast Sessions area appears at the bottom of the window.



8 In the **Maximum Unicast Sessions** box, type the maximum number of simultaneous unicast sessions that you want the server to allow.

Note: The value that you type in this box is used to limit the number of client sessions and, as a result, the network bandwidth usage. Since each open display adds CPU load on the application server, and adds to the overall bandwidth usage on the network, you must limit the number of client sessions by typing the number in this box. Once this limit is reached, no further unicast real-time connections are accepted until one of the existing streams is closed. An error message is logged on the application server to indicate the limit was reached, and a message appears on the client, indicating that the connection is not allowed. For guidance on entering the appropriate value, refer to “Unicast LAN/WAN impact” on page 39.

9 Click the **Restart Real Time Reporting Service** check box so that it is checked.

10 Click **OK**.

Result: The Restart ICERtdService status window appears while the service is restarting, and closes once the service has restarted successfully.

11 Click Console → Exit to close the Nortel Networks Applications Configuration window.

What's next?

Configure Emergency Help on the application server. See "Configuring Emergency Help" on page 173 for more information.

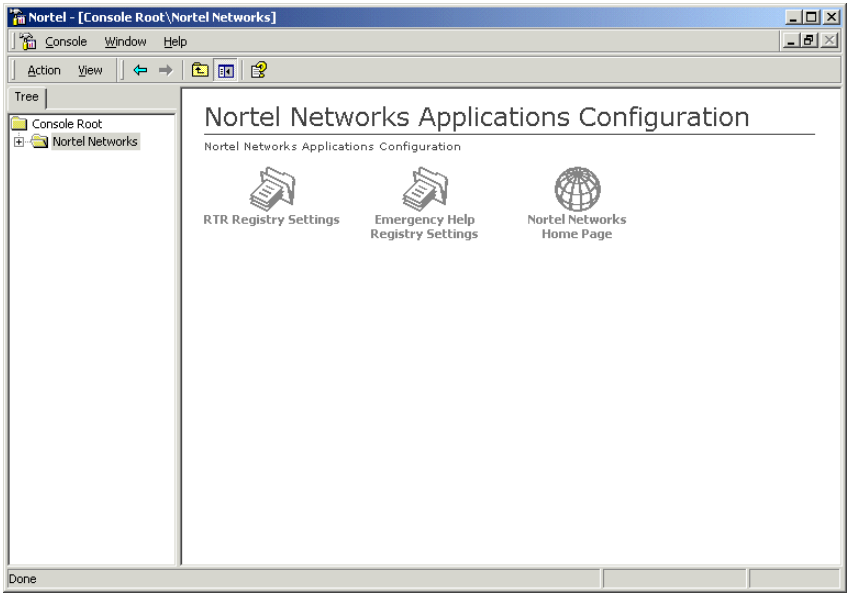
Configuring Emergency Help

To configure Emergency Help

Note: The Emergency Help component only functions if you are using the multicast communication method from the application server to the client PC.

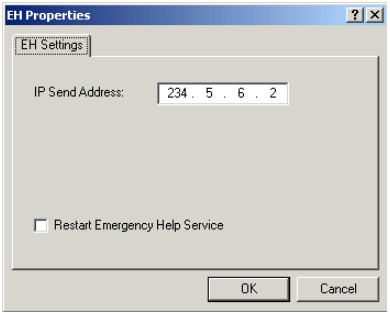
1 Click Start → Programs → Symposium Web Client → Configuration.

Result: The Nortel Networks Applications Configuration window appears.



2 Click the **Emergency Help Registry Settings** icon.

Result: The EH Properties window appears.



3 In the **IP Send Address** box, type the IP address to which the Symposium Web Client application server sends Emergency Help information. This IP Send address can be the same as or different from the IP address that the application server uses to send Real-Time Reporting and Agent Desktop Displays data to client PCs. Consult the “Pre-installation worksheet” on page 537 to verify the IP Send address that you chose for the application server to send Emergency Help data to client PCs (item 16 of the worksheet).

4 Click the **Restart Emergency Help Service** check box.

5 Click **OK**.

If you do not click the Restart Emergency Help Service check box, the system prompts you to do so.

What’s next?

Configure Historical Reporting on the application server. See “Configuring Historical Reporting” on page 175 for more information.

Configuring Historical Reporting

Introduction

To ensure that the Historical Reporting component functions properly in the Symposium Web Client application, you must complete the following tasks:

- Verify that SMTP is installed.
- Configure SMTP.
- Set up a default printer on the application server.
- Set up a shared folder for exporting files.

When the Historical Reporting component generates a scheduled report, it can send an e-mail notification to report recipients. To ensure that Historical Reporting sends an e-mail to the appropriate individual when a report is ready, you must install and configure a Simple Mail Transfer Protocol (SMTP) server on the application server.

Note: To use SMTP, Internet Information Services (IIS) and Microsoft Active Directory must be installed on the application server. For more information, see "System requirements" on page 26.

To verify that an SMTP server is installed

1. Click Start → Programs → Administrative Tools → Internet Services Manager.

   Result: The Internet Information Services window appears.

2. Click the plus sign (+) beside the name of the Symposium Web Client application server.

   Result: If one of the branches that appears on the application server tree is Default SMTP Virtual Server, then an SMTP server is installed.

Once you have verified that SMTP is installed, you can configure the SMTP server to send e-mail notifications from Historical Reporting.

To configure the SMTP server

To configure the SMTP server, you must provide a domain name and a host name to indicate where Web Client should send e-mail notifications.

1 Click Start → Programs → Administrative Tools → Internet Services Manager.

Result: The Internet Information Services window appears, displaying the domain tree in the left pane.

2 Click the plus sign (+) beside the name of the Web Client application server to expand the application server tree.

3 Right-click the Default SMTP Servers branch, and then select **Properties** from the resulting pop-up menu.

Result: The Default SMTP Virtual Server Properties window appears.

4 Click the **Delivery** tab.

5 Click **Advanced**.

Result: The Advanced Delivery window appears.

6 In the **Fully qualified domain name** box, type the domain name of the Web Client application server:

***<computername>.<computername>.<domain name>*.com**

Example: pcbox123.pcbox123.softwarehouse.com

7 Click **Check DNS** to validate the domain name.

8 In the **Smart Host** box, type the host name of the Microsoft Exchange server.

Note: The Smart Host name should be the name of a valid mail server. If you are unsure of the name of your mail server, and your company uses Microsoft mail server software, you can check the name of your mail server by opening the Mail dialog box in Control Panel on a client PC with e-mail services.

a. Click Start → Settings → Control Panel.

b. Double-click the **Mail** icon.

Result: An MS Exchange Settings Properties dialog box appears.

c. Click the **Services** tab.

d. In **The following information services are set up in this profile** section, click **Microsoft Exchange Server**.

e. Click **Properties**. The Microsoft Exchange Server dialog box appears. The name of the mail server appears in the Microsoft Exchange server box.

9 Click the **Attempt direct delivery before sending to smart host** check box.

10 Click the **Perform reverse DNS lookup on incoming messages** check box.

11 Click **OK** to close the Advanced Delivery window.

12 Click the **Access** tab.

13 Click **Authentication**.

14 Deselect the check mark in the **Basic authentication** check box.

15 Click **OK** to close the Authentication window.

16 Click the **Connection** tab.

Result: The Connection window appears.

17 Click **All except the list below**.

18 Click **OK**.

19 If you want to track commands that are sent over the network from SMTP client PCs to the SMTP virtual server, perform the following steps:

a. Click the **General** tab.

b. Click the **Enable logging** check box.

c. Select a format from the **Active log format**.

20 Click the **Message** tab.

21 Ensure all check boxes are checked.

22 In the **Send copy of Non-Delivery report to** box, type the e-mail address of the person who monitors the Non-Delivery report.

23 Click **OK** to close the Default SMTP Virtual Server Properties window.

To set up a default printer

There are two procedures for you to choose from when setting up a printer to print scheduled historical reports and scripts. You can add

- a network printer that has its own IP address
- a network shared printer that is connected to a print server other than the application server

Choose the procedure that is most appropriate for your organization.

To set up a default network printer that has its own IP address

To use a network printer to print scheduled reports from the Historical Reporting component and scripts from the Scripting component, you must add and configure the printer on the application server while logged on as the administrator.

If you require additional information on adding printers, contact Microsoft or your network administrator, or consult your Microsoft documentation. The procedure that you need to use depends on the network configuration of your call center. Consult your Microsoft documentation or the online Help in Windows 2000 for proper printer setup and configuration. Click Start → Programs → Administrative Tools → Configure Your Server → Print Server → Learn More, and then type **Choosing and configuring a port** in the Search box.

The following procedure is valid for network printers that have a standard TCP/ IP protocol, or that use a Hewlett-Packard Jet Direct card.

1 Click Start → Settings → Printers.

Result: The Printers window appears.

2 Double-click the **Add Printer** icon.

Result: The Add Printer window appears.

3 Click **Next**.

Result: The Local or Network Printer window appears.

4 Accept the default so that **Local Printer** is selected.

5 Deselect the **Automatically detect and install my Plug and Play printer** check box.

6 Click **Next**.

Result: The Select the Printer Port window appears.

7 Select **Create a new port**.

8 From the **Type** drop-down list, select **Standard TCP/IP Port**.

9 Click **Next**.

Result: The Welcome to the Add Standard TCP/IP Port Wizard window appears.

10 Click **Next**.

Result: The Add Port window appears.

11 In the **Printer Name or IP address** box, type the printer IP address.

Result: The system populates the **Port Name** box with the appropriate port name.

12 Click **Next**.

Result: The Completing the Add Standard TCP/IP Printer Port Wizard window appears.

13 Click **Finish**.

Result: After a few moments, the Add Printer Wizard window reappears.

14 In the **Manufacturer** and **Printer** boxes, select the appropriate information for your printer.

15 Click **Next**.

Result: The Name Your Printer window appears.

16 Type the printer name.

Result: The Printer Sharing Window appears.

17 Accept the default with **Share as** selected.

18 Click **Next**.

Result: The Location and Comment window appears.

19 Type information in the **Location** box and **Comment** box (optional).

20 Click **Next**.

Result: The Print Test Page window appears.

21 Click **Yes** to print a test page.

Result: The Completing the Add Printer Wizard window appears.

22 Click **Finish**.

To set up a network shared printer connected to a print server other than the application server

The following procedure outlines how to set up a default network printer that is connected to a print server other than the application server (for example, a UNIX server). You perform the procedure on the application server by pointing to the print server on your network.

Note: If the print server is a UNIX computer, you must select an LPR port when configuring the printer on the application server. If the LPR port is not among the options listed in the Add Printer wizard, you must first install Print Services for UNIX on the application server. You can install this utility from the Windows 2000 Server CD by clicking Add/Remove Programs → Windows Components → Other Network File and Print Services. Click **Details,** and in the resulting dialog box, select **Print Services for Unix**. Click **OK** to install the utility. When the installation is complete, proceed with adding the default printer.

1 Click Start → Settings → Printers.

Result: The Printers window appears.

2 Double-click the **Add Printer** icon.

Result: The Add Printer Wizard appears.

3 Click **Next**.

Result: The Local or Network Printer window appears.

4 Accept the default so that **Local Printer** is selected.

5 Clear the **Automatically detect and install my Plug and Play printer** check box.

6 Click **Next**.

Result: The Select the Printer Port window appears.

7 Click **Create a new port**.

8 From the Type drop-down list, select **LPR port**.

9 Click **Next**.

Result: The Add LPR Compatible Printer window appears.

10 In the **Name or address of server providing lpd** box, type the DNS name or IP address of the print server.

11 In the **Name of printer or print queue on that server** box, type the name of the printer as it is identified by the host, which is either the direct-connect printer or the UNIX computer.

12 Click **OK** to close the window and return to the Wizard.

13 Follow the remaining prompts in the wizard to finish installing the printer.

To export files from Historical Reporting

To the application server

To export scheduled report files to the application server, in the Output box on the Report Properties window, type the path to the shared folder where the report will be output. The path must have the format \\[application server name]\[shared folder name]\[file name], without the file extension.

Example: You want to output the Agent Performance report to a shared folder on the application server. The application server computer name is *appsrvr*, the shared folder name is *reports*, and you decide to call the report *agent*. You type **\\appsrvr\reports\agent** in the Output box.

To enable users to access the saved report file, you must grant each user read/delete access rights to this folder on the application server (or alternately, create separate shared folders with read/delete access for each applicable user). For details on configuring user access privileges, see the Microsoft Windows 2000 Server documentation.

To a client PC

You can only export files to client PCs that are within the same domain as the application server. To output scheduled report files to a client PC, in the Output box on the Report Properties window, type the path to the shared folder where the report will be output. The path must have the format \\[client PC computer name]\[shared folder name]\[file name], without the file extension.

When you create the shared folder on the client PC where the application server can send the output file, you must map to this folder from the application server. You must also grant write access privileges to this folder for *Everyone*. For details on configuring user access privileges, see the Microsoft Windows 2000 Server documentation.

If you require additional information on creating and mapping folders, see your Microsoft documentation.

Note: The combined number of ad hoc or scheduled reports that you can generate simultaneously is limited to five. You can schedule as many historical reports as required; however, only five scheduled reports are processed simultaneously while the others wait in queue. Likewise, for ad hoc reports, only five reports can be generated at the same time. For example, five supervisors can generate an ad hoc report, but the sixth supervisor to do so receives a message saying the system could not process the request. This supervisor must try to generate the ad hoc report again later, after the first five reports have been generated (or schedule the report to run later). This limitation applies to the *total* of the ad hoc and scheduled reports that can be generated at a particular time. For example, if two reports are scheduled to be output at noon, then only three ad hoc reports can be generated at this time, bringing the total to five.

What's next?

Configure Scripting on the application server. See "Configuring Scripting" on page 183 for more information.

Configuring Scripting

Introduction

To use the Scripting component, you must perform the following procedures:

- Configure the Terminal Services user account in Active Directory.
- Provide access rights to the Scripting component.
- Configure Terminal Services.
- Activate the Terminal Services License Server.
- Set up a default printer on the application server.

Accessing Scripting

To access the Scripting component, users must connect to the application server using Terminal Services. You must configure a unique Terminal Services user account in Active Directory, and grant this user certain access rights and permissions to the Scripting component that resides on the application server.

ATTENTION

As of date of publication, the following information on Client Access Licensing was available from Microsoft. Consult Microsoft for the latest information. Nortel Networks does not accept any liability for end-user compliance with Microsoft licensing agreements. This information has been provided for your convenience.

- You must purchase from Microsoft both a Terminal Services Client Access License and a Windows 2000 Server Client Access License for each client PC running on Windows 98 or NT that will be accessing the Script Manager portion of the Scripting component.
- Client PCs running on Windows 2000 or Windows XP require a Windows 2000 Server Client Access License only; they do not require a separate Terminal Services Client Access License.
- Nortel Networks does not provide these Client Access Licenses.
- The Windows 2000 Server Client Access Licenses do not float (that is, they are specific to the client PCs for which they have been purchased).
- If the client PC is accessing only Script Variables or Application Thresholds, then these licenses are not required.

To configure the Terminal Services user account in Active Directory

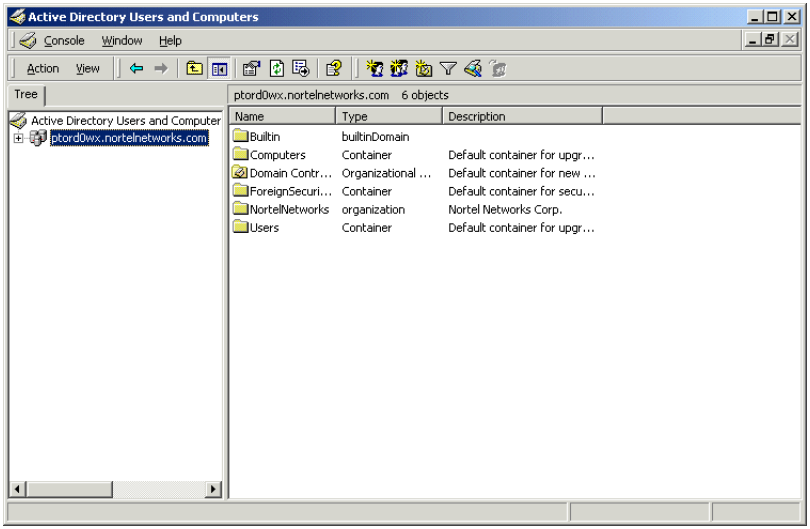
The following procedure creates the TsInternetUser account in Active Directory, an account that enables all users who have access to the Terminal Services Client to log on to Terminal Services on the application server without entering a user ID or password.

If you want to create a more secure environment for this component, you can create one or more accounts of your choice in Active Directory and require that users enter both a user ID and password, or only a password for these accounts each time they log on to the Scripting component. For more information, see "Configuring Terminal Services in a secure environment" on page 271.

Note: If you create a more secure environment by creating and using the Active Directory account of your choice, then Nortel Networks recommends that you disable the TsInternetUser account. For more information, see "To disable the TsInternetUser account" on page 285.

1 Click Start → Programs → Administrative Tools → Active Directory Users and Computers.

Result: The Active Directory Users and Computers window appears.



2 In the **Tree** tab, click the plus sign (+) beside the application server's domain name to expand the tree, and then click the Users folder.

3 On the **Name** column, right-click the user name **TsInternetUser**, and then select All Tasks → Reset Password.

Result: The Reset Password window appears.

4 In the **New Password** and **Confirm Password** boxes, type the **TsInternetUser** password.

5 Ensure that the **User must change password at next logon** check box is unchecked.

Note: Leave the **Domain Name** box blank.

6 Click **OK**.

Result: The Active Directory confirmation box appears, confirming that the TsInternetUser password has changed.

7 Click **OK** to close the window.

8 In the Active Directory Users and Computers window, right-click **TsInternetUser** and select **Properties**.

Result: The TsInternetUser Properties window appears.

9 Click the **Member Of** tab.

10 In the **Member of** list box, select **Guests**, and then click **Remove**.

Result: The Remove user from group confirmation box appears.

11 Click **Yes**.

12 Click **Apply**.

13 Click **OK** to close the window.

14 In the Active Directory Users and Computers window, click Console → Exit to close the window.

To provide access rights to the Scripting component

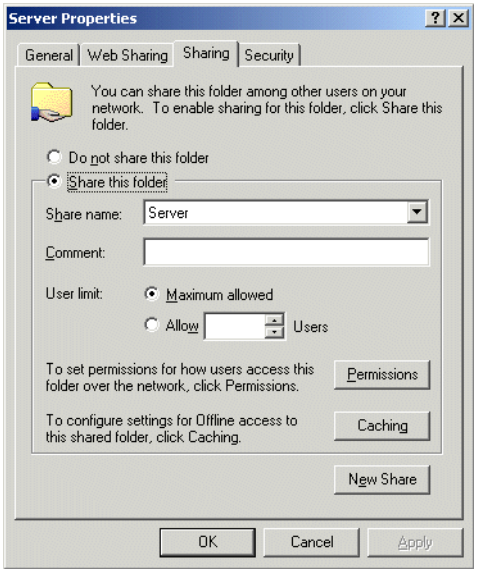
1 Navigate to the following folder:

***c:*\Program Files\Nortel Networks\WClient\Server**

where *c:* is the drive in which Symposium Web Client is installed.

2 Right-click the **Server** folder, and then select **Properties** from the resulting pop-up menu.

3 Click the **Sharing** tab.

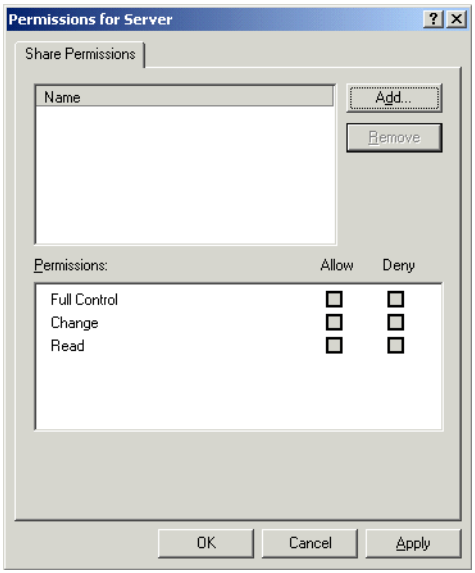


4 Click **Share this folder**.

5 In the **Share name** box, confirm the folder name.

6 Click **Permissions**.

Result: The Permissions for Server window appears.



7 Click **Add**.

Result: The Select Users, Computers or Groups window appears.

8 From the list of users, select **TsInternetUser**.

9 Click **Add**.

Result: The TsInternetUser is added to the box in the lower half of the window.

10 Click **OK** to close the window.

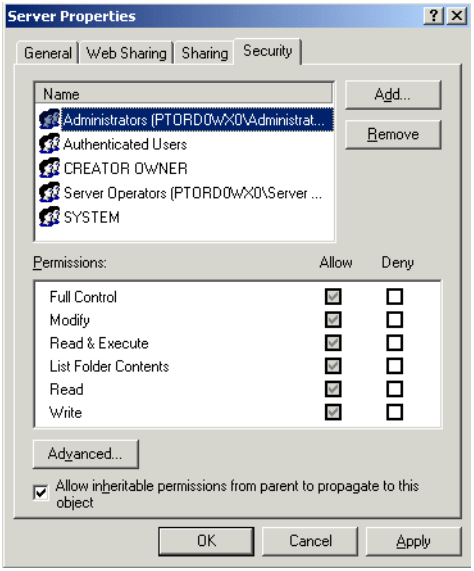
11 In the Permissions for Server window, select **TsInternetUser**.

12 In the **Permissions** box, click the **Read** check box in the **Allow** column to ensure that the TsInternetUser has read-only access.

13 Click **Apply**.

14 Click **OK** to close the window.

15 Click the **Security** tab.



16 Click **Add**.

Result: The Select Users, Computers or Groups window appears.

17 Select **TsInternetUser**.

18 Click **Add**.

Result: The user name TsInternetUser appears in the lower half of the window.

19 Click **OK** to close the window.

20 In the Server Properties window, select **TsInternetUser**.

21 In the **Permissions** box, click all check boxes in the **Allow** column to ensure that the TsInternetUser has full access.

22 If the **Everyone** group appears in the top of this window, highlight this group.

23 Click **Remove**.

Note: Based on the type of Symposium Web Client installation that you have performed, the Everyone group may not appear in this window. If you have performed a fresh installation of the software, then this group does not

appear; however, if you have upgraded Symposium Web Client from a previous release this group may appear, in which case, you must remove it.

24 Click **Apply**.

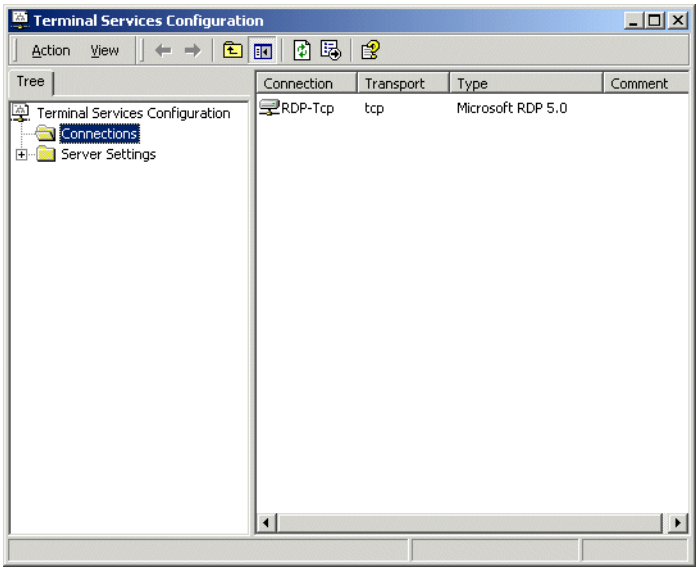
Note: The TsInternetUser account must have Read access to the Server folder. If you select the check box beside **Allow inheritable permissions from parent to propagate to this object**, then the Server folder inherits the access permissions of its parent folder. Based on the permissions you have set on the parent folder, therefore, you can select this check box on this tab, but only if it does not deny Read access to the Server folder for the TSInternetUser account. All permissions you select on this tab take precedence over those you selected on the Sharing tab.

25 Click **OK** to close the window.

To configure Terminal Services

1 Click Start → Programs → Administrative Tools → Terminal Services Configuration.

2 The Terminal Services Configuration window appears.



3 Double-click the **RDP-Tcp** icon in the right side of the window.

Result: The RDP-Tcp Properties window appears.

4 Click the **Logon Settings** tab.

5 Click **Always use the following logon information**.

6 In the **User name** box, type **TsInternetUser**.

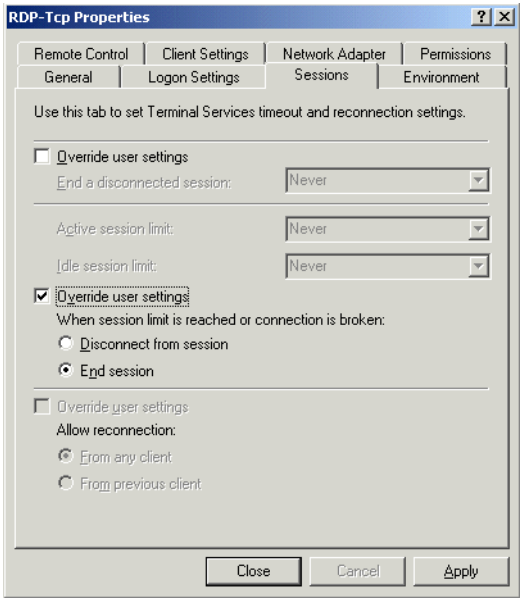
7 Deselect **Always prompt for password** to remove the check mark.

Note: By deselecting **Always prompt for password**, users accessing the Script Manager/Editor will not be prompted for the user ID and password. However, if you are concerned about security, you may want to select this option to restrict client PCs with the Terminal Services Client application from directly accessing the application server. When you select **Always prompt for password**, the system prompts all users to enter the user ID and password each time they start the Script Manager/Editor.

8 In the **Password** and **Confirm password** boxes, type the password you created in step 4 on page 186.

9 Click **Apply**.

10 Click the **Sessions** tab.



11 Click the *second* **Override user settings** check box, and then click **End session**.

12 Click **Apply**.

13 Click **Close**.

14 Exit the Terminal Services Configuration window.

To activate the Terminal Services License Server

The installation of Terminal Services provides you with the Terminal Services software for a 90-day evaluation period only. Before the 90 days expire, you must purchase a Terminal Services license, as described in the Terminal Services Licensing paragraph from Microsoft, to continue to use the Scripting component beyond the evaluation period. To ensure that the licensed clients can continue to access Scripting beyond this period, you must also activate the Terminal Services License Server on the application server with a license server ID provided by Microsoft.

1 On the application server, click Start → Programs → Administrative Tools → Terminal Services Licensing.

Result: The Terminal Services Licensing window appears.

2 In the window, right-click the application server icon, and then choose **Activate Server** from the pop-up menu.

Result: The Licensing Wizard starts.

3 Follow the prompts in the wizard to connect to Microsoft, obtain the license server ID, and activate the License Server.

To set up a default printer for Scripting

To print scripts while using the Web Client Scripting component, you must first configure a local printer on the application server while logged on to Windows 2000 as the administrator. For detailed information on this procedure, see “To set up a default printer” on page 178.

To export scripts

To the application server

To export scheduled script files to the application server, you must create a shared folder on the server. Then, to enable users to access the saved script file, you must grant each user read/delete access rights to this folder on the application server (or alternately, create separate shared folders with read/delete access for each applicable user). For details on configuring user access privileges, see the Microsoft Windows 2000 Server documentation.

To a client PC

You can only export scripts to client PCs that are within the same domain as the application server. To export script files to a client PC, you must create a shared folder on the client PC where the application server can send the script file. You must grant write access privileges to this folder for *Everyone*. Then, you must map to the client PC's shared folder from the application server. For details on configuring user access privileges, see the Microsoft Windows 2000 Server documentation.

If you require additional information on creating and mapping folders, see your Microsoft documentation.

What's next?

Configure Agent Desktop Displays on the application server. For more information, see "Configuring Agent Desktop Displays" on page 194.

Configuring Agent Desktop Displays

Introduction

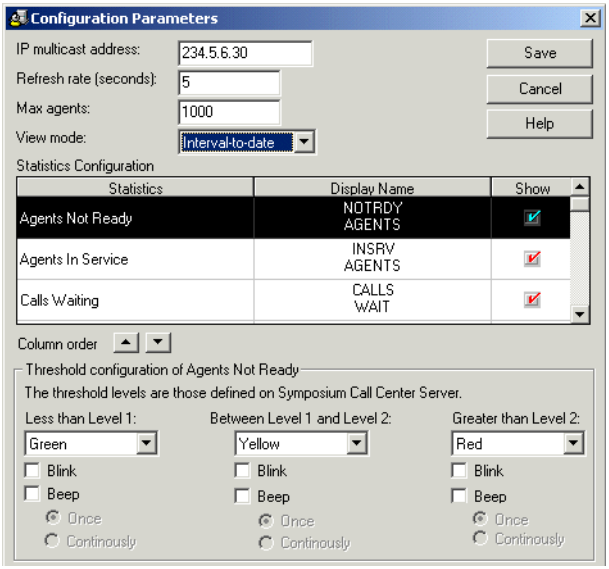
Note: The Agent Desktop Displays component only functions if you are using the multicast communication method from the application server to the client PC.

To use Agent Desktop Displays on a client PC, you must configure the parameters on the application server. You must also have the Real-Time Reporting component installed and configured on the application server for Agent Desktop Displays to function properly.

To configure Agent Desktop Displays

1 Click Start → Programs → Symposium Agent Displays → Server Configuration Parameters.

Result: The Configuration Parameters window appears.



2 Confirm that the address in the **IP multicast address** box is the application server's IP send address that you configured in the RTR Configuration Tool. For more information, see "Configuring Real-Time Reporting" on page 165.

3 In the **Refresh rate (seconds)** box, type the rate in seconds at which you want the real-time data in the displays to be refreshed.

Note: The minimum value that you can type in this field is 2 seconds. If you do not type a value in this box, the system uses the default value of 5 seconds.

4 In the **Max agents** box, type the maximum number of agents who can simultaneously log on to the Symposium Agent Desktop Displays component and view the real-time statistics.

Note: When the number of agents who have logged on to the application reaches this number, any additional agents who try to log on will receive a message informing them to try again later. If you do not type a value in this box, the system uses the default value of 1000 agents. The maximum value that you can type in this box is 3000 agents.

5 In the **View mode** drop-down list, select the mode in which you want to view the data that has been collected:

- **Moving window**: In moving window mode, statistics shown represent the last 10 minutes of system activity.
- **Interval-to-date**: In interval-to-date mode, statistics are collected only for the current interval. When the interval is over, data fields reset to 0 and collection begins for the next interval. The interval can correspond to a work shift or to another system-defined period.

6 In the **Statistics Configuration** table, choose the statistics that you want to appear in the Agent Desktop Displays. You can add statistics columns to the displays, or remove columns that you no longer want to show.

7 Click the check box in the **Show** column if you want to add the statistics column to the displays.

8 Arrange the order in which the statistics columns will appear by using the column order buttons. Select the statistic that you want to move, and then click the up or down button to change its position.

Note: The statistic that you place at the top of the **Statistics Configuration** table appears in the first column of the display.

9 Select the three threshold colors for the selected statistic from the Threshold display colors drop-down lists. Select the statistic and use colors to identify whether the value of the statistic shown in the display is less than

the low value, between the low and high value, or greater than the high value.

Note: If you have not set the threshold levels in the Configuration component of Web Client or in Symposium Call Center Server, the values appear in white in the Symposium Agent Desktop Displays.

10 Click the **Blink** check box if you want the selected statistic to blink in the Agent Desktop Display when its value reaches the threshold.

11 Click the **Beep** check box if you want the Agent Desktop Display to beep when its value reaches the threshold.

12 Click **Once** to indicate that a beep should occur only once, or click **Continuously** to indicate that a beep should occur continuously until the statistic reaches an acceptable value.

13 Click **Save**.

What's next?

Configure the application server for optimum security. For more information, see Section F: "Security and the application server" on page 197.

Section F: Security and the application server

In this section

Overview 198
Removing the Everyone group from the application server 200
Installing, configuring, and uninstalling IIS Lockdown and URLScan 207
Changing the default anonymous Internet Guest account 248
Disabling the parent path in IIS 263
Enabling Secure Sockets Layer on the application server 266
Configuring Terminal Services in a secure environment 271

Overview

Introduction

To help safeguard the Symposium Web Client application server against security threats, such as unauthorized individuals trying to access restricted information or authorized users accidentally altering/deleting files, you must identify and configure the correct security settings for the server.

Where possible, Symposium Web Client aims to adhere to Microsoft's published guidelines on securing Internet Information Server (IIS). However, since security policies vary from organization to organization, it is impossible to provide security recommendations that suit all businesses. The following security recommendations conform to best practice policies where possible, within the scope of the technology being used.

Note: This section includes steps that you can perform to increase the level of security on the Symposium Web Client application server. In particular, it details security measures related to the setup and configuration of Internet Information Server (IIS) on the application server; it does not include information on security issues that are external to the application server (for example, firewall setup and configuration).

Security procedures included in this section

This section includes the following optional security procedures:

- removing the Everyone group
- configuring and enabling IIS Lockdown and URLScan
- changing the anonymous Internet Guest Account
- disabling the parent path in IIS
- enabling Secure Sockets Layer (SSL) on the application server
- configuring Terminal Services in a secure environment

Notes:

- For security information related to cookies, see “To configure Internet Explorer 6.0 Service Pack 1 (or later)” on page 297.
- To ensure that your Internet browser cache settings are set correctly, follow the appropriate procedure for configuring your version of Internet Explorer. See either “To configure Internet Explorer 5.5 Service Pack 2 (or later)” on page 294, or “To configure Internet Explorer 6.0 Service Pack 1 (or later)” on page 297 for details.

Removing the Everyone group from the application server

Introduction

When you install Windows 2000 Server/Advanced Server on the application server, the default configuration includes full control permissions on all disk drives for the Everyone group. This means that anyone who can access the server is granted full control permissions to all files and folders on all disk drives, which poses a security risk to the application server. To further secure the application server, you can remove the Everyone group from all of the server's disk drives after you install the Symposium Web Client software. This is an optional procedure.

Since the system requires that there be at least one Windows user account or group with full control permissions to function properly, you must add and configure this group or user before you delete the Everyone group. Failure to do so may cause the operating system or Symposium Web Client to malfunction.

The procedure for removing the Everyone group involves the following main steps:

- On all system drives, add and configure three groups with full control permissions: Administrators, SYSTEM, and Domain Admins.
- On the drive where Symposium Web Client is installed, add and configure one user account with Read & Execute, Modify, and Write permissions (the IUSR_<*computer name*> user account) and another user account with only Read & Execute permissions (the IWAM_<*computer name*> user account), where <*computer name*> is your server's computer name.
- On the drive where the operating system is installed, add and configure the TsInternetUser account with Read & Execute permissions.
- On the desired drives, add and configure any additional user accounts and groups, as required by your organization's security policy.
- On all system drives, remove the Everyone group.

ATTENTION

If you have created a new account to replace the default TsInternetUser account for Terminal Services, then you must use this new account wherever the TsInternetUser account is listed in the following procedure.

Likewise, if you have changed or created a new IUSR_<*computer name*> user account to satisfy your company's security policies, then you must use this new account throughout the following procedure wherever it lists the IUSR_<*computer name*> user account. For information on changing this account or creating a new account, see "Changing the default anonymous Internet Guest account" on page 248.

Note: If you perform the following procedure with the default IUSR_<*computer name*> user account, and then you subsequently disable this account in the "Changing the default anonymous Internet Guest account" procedure, then the settings you configure here will be lost.

To remove the Everyone group from the application server

1. Log on to the application server using the administrator account.
2. Click Start → Programs → Accessories → Windows Explorer.
3. In the left pane of Windows Explorer, double-click My Computer.
4. Right-click the drive on which the Symposium Web Client application is installed (for example, drive C). From the resulting pop-up menu, click **Properties**.

   Result: The Local Disk (*drive letter*) Properties window appears.
5. Click the **Security** tab.
6. Click **Add**.

   Result: The Select Users, Computers, or Groups window appears.

7 While holding down the Ctrl key, from the list of groups and user accounts, click the following groups. Groups are denoted by the double-head icon; user accounts have the single-head icon:

- **Administrators**
- **SYSTEM**
- **Domain Admins**

8 Click **Add**.

Result: These groups appear at the bottom of the window.

9 While holding down the Ctrl key, from the list of groups and user accounts, click the following user accounts. Groups are denoted by the double-head icon; user accounts have the single-head icon:

- IUSR_<*computer name*>
- IWAM_<*computer name*> (where <*computer name*> is your server's computer name)

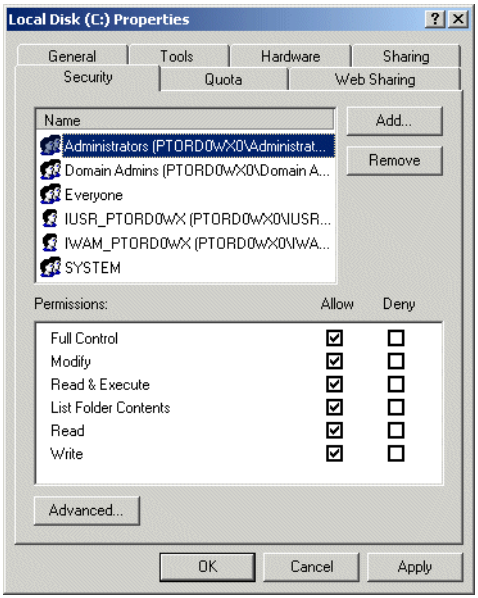
10 Click **Add**.

Result: These user accounts appear at the bottom of the window, along with the three group accounts you have already chosen.

11 Click **OK** to transfer these accounts to the properties window, where you can configure their permissions on the server drive that you have chosen.

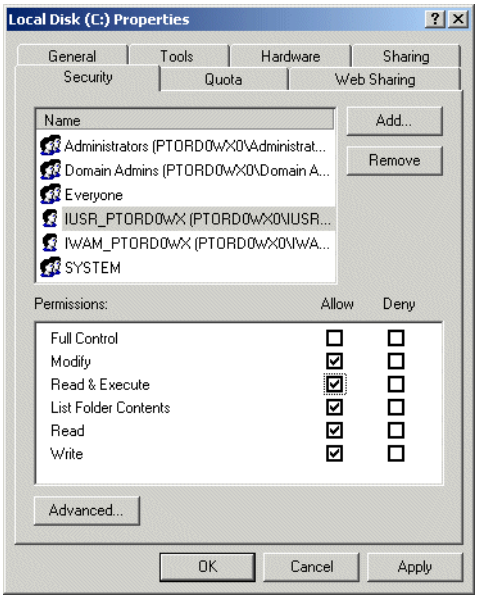
12 In the Name box, highlight *each* of the three new groups you added (**Administrators**, **Domain Admins**, and **SYSTEM**), and then click the

check box beside **Full Control** under the Allow column heading, as shown in the following graphic:



13 In the Name box, highlight the first new user account you added, **IUSR_*<computer name>*** , and then ensure there is a check mark beside

Read & Execute, **Modify**, and **Write** under the Allow column heading, as shown in the following graphic:

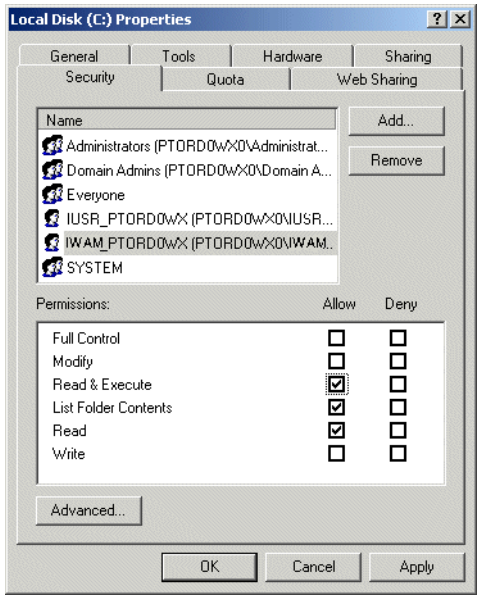


Note: When you select **Allow** beside Read & Execute, it automatically includes List Folder Contents and Read permissions.

14 Click **Apply**.

15 In the Name box, highlight the other new user account you added, **IWAM_*<computer name>***, and then ensure there is a check mark beside

Read & Execute under the Allow column heading, as shown in the following graphic:



Note: When you select **Allow** beside Read & Execute, it automatically includes List Folder Contents and Read permissions.

16 Click **Apply** to save your changes.

17 Add additional user accounts and groups in the same manner, as required by your organization's security policy. If you do not need to add any additional user accounts or groups, proceed to the next step.

18 While in the properties window, highlight the **Everyone** group, and then click **Remove**.

19 Click **OK** to save your changes and close the properties window.

20 To add the TsInternetUser account, in Windows Explorer, right-click the drive on which the operating system is installed (for example, drive C). From the resulting pop-up menu, click **Properties**.

Result: The Local Disk (*drive letter*) Properties window appears.

21 Click the **Security** tab.

22 Click **Add**.

Result: The Select Users, Computers, or Groups window appears.

23 From the list of groups and user accounts, click the **TsInternetUser** account. (User accounts have the single-head icon.)

24 Click **Add**.

25 The user account appears at the bottom of the window.

26 Click **OK** to transfer the account to the properties window, where you can configure its permissions on this drive.

27 In the **Name** box, highlight the TsInternetUser account, and then click the check box beside Read & Execute under the Allow column heading.

Note: When you select **Allow** beside Read & Execute, it automatically includes List Folder Contents and Read permissions.

28 While in the properties window, if you have not already removed the Everyone group from the currently selected drive, highlight the **Everyone** group, and then click **Remove**.

29 Click **OK** to save your changes and close the properties window.

30 If there are additional disk drives on the application server (for example, if the operating system is installed on a different drive than the Symposium Web Client software), then you must add the **Administrators**, **Domain Admins**, and **SYSTEM** groups with full control permissions to these drives, and remove the **Everyone** group, according to the preceding steps. You must also add any additional user accounts and groups required by your organization's security policy to these drives.

Note: You do not need to add and configure the **IUSR_*<computer name>*** and **IWAM_*<computer name>*** user accounts on any other drives but the drive containing the Symposium Web Client software.

31 When you are finished, click **OK** to save your changes and close the properties window.

Installing, configuring, and uninstalling IIS Lockdown and URLScan

Introduction

ATTENTION

For proper Symposium Web Client functionality, you must install the Symposium Web Client software before performing the IIS Lockdown procedure. However, if you had already installed IIS Lockdown before installing Symposium Web Client, then you must follow a series of steps to uninstall IIS Lockdown and recover the application server. For more information, see “To uninstall IIS Lockdown and reconfigure an application server that was installed as the default web site” on page 226, or “To uninstall IIS Lockdown and reconfigure an application server that was installed as part of an existing site” on page 234.

When you perform the IIS Lockdown procedure, the system takes a backup of IIS and all configured virtual folders. The Symposium Web Client installation creates new virtual folders. Therefore, if you perform the IIS Lockdown before installing the Symposium Web Client software, it does not back up these new virtual folders.

If the Symposium Web Client virtual folders are not included in the backup, it creates problems when uninstalling IIS Lockdown. During the uninstall, IIS Lockdown restores IIS from its backup copy. If the backup does not contain the Symposium Web Client virtual folders, then these folders do not appear after you uninstall IIS Lockdown, causing Symposium Web Client to malfunction.

The following two Microsoft tools enable you to add additional security features to an IIS web server, such as the application server:

- IIS Lockdown
- URLScan

The procedure in this section illustrates how to download and install the IIS Lockdown tool, including the URLScan feature. This is an optional procedure that enables you to further secure the application server.

How IIS Lockdown works

IIS Lockdown works by turning off unnecessary features, such as the news service or the file transfer service, thereby reducing potential IIS attack points. To install IIS Lockdown, you must download the installation wizard from the Microsoft web site at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/locktool.asp. You can then run the installation from the web site, or save the installation file, *iislokd.exe*, to the application server's hard drive for later installation.

IIS Lockdown and URLScan

When you install IIS Lockdown according to the following procedure, you also install the URLScan component. URLScan is another Microsoft tool that can provide additional security when used in conjunction with IIS Lockdown. It restricts the type of HTTP requests that the server will process, and the types of file transfers that are allowed to and from the server. For example, when the IIS Lockdown feature is enabled, URLScan does not allow users to download files with the .exe extension from the application server.

For more information on either of these features, see http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/locktool.asp on the Microsoft web site.

Note: Since the Symposium Configuration spreadsheets have the .exe extension, administrators cannot download these spreadsheets when the IIS Lockdown and URLScan features are enabled. Therefore, you must enable IIS Lockdown and URLScan only *after* users have downloaded the spreadsheets. Should you need

to download a spreadsheet (or another .exe file) while IIS Lockdown is enabled, then you can *temporarily* alter the urlscan.ini file to allow this activity, provided that it conforms to your company's security policy. For more information, see "To temporarily edit the urlscan.ini file" on page 224.

IIS Lockdown and Symposium Web Client upgrades

If you are upgrading your application server from Symposium Web Client Release 4.0 with IIS Lockdown installed to Symposium Web Client Release 4.5, then you must perform the following series of steps:

- Uninstall IIS Lockdown.
- Install Symposium Web Client Release 4.5.
- Reinstall IIS Lockdown.

IIS Lockdown and the application server

The risk of IIS security vulnerability on the Symposium Web Client application server is minimal for the following reasons:

- The application server's IIS component is only used for the Symposium Web Client application and is not shared with other web applications.
- The application server's IIS component should only be used within the customer's intranet environment and is not exposed to a regular Internet environment.
- Anyone who accesses the Symposium Web Client IIS contents must first go through valid Web Client user logon and password authentication.

In spite of these inherent security features, Nortel Networks acknowledges that some customers have security policies that may require that IIS Lockdown and URLScan be installed and configured on the application server.

IIS Lockdown and the MSADC virtual directory

The procedure for installing and configuring IIS Lockdown in this section includes the removal of the MSADC virtual directory, which disables the Remote Data Service (RDS) form of communication. In Symposium Web Client 4.5, you can disable RDS because the application server uses the Simple Object Access Protocol (SOAP) communication method instead.

However, before you disable RDS by removing the MSADC virtual directory, you must verify the following:

- *All* client PCs connecting to the Symposium Web Client 4.5 application server must have SOAP 3.0 installed.
- *All* client PCs connecting to the application server to view the Agent Desktop Displays must have the Agent Desktop Displays 4.5 installed.

Note: The Agent Desktop Displays software that is installed with Symposium Web Client 4.0 is called Agent Desktop Displays 4.0. The Agent Desktop Displays software that is installed with Symposium Web Client 4.5 is called Agent Desktop Displays 4.5.

When you use the Agent Desktop Displays 4.0 with Symposium Web Client 4.5, the communication between the client PC and application server is through RDS, not SOAP. In this case, therefore, you *cannot* remove the MSADC virtual directory through the IIS Lockdown procedure because it disables RDS, which causes Agent Desktop Displays 4.0 to malfunction. Instead, you can perform the IIS Lockdown procedure, but leave the MSADC virtual directory enabled.

Alternately, if you have already disabled RDS through the IIS Lockdown procedure, then you must reenable it before you can use Agent Desktop Displays 4.0 with Symposium Web Client 4.5. For more information, see “To reenable Remote Data Service” on page 244.

Once all Agent Desktop Displays clients have been upgraded to Release 4.5 (and have SOAP 3.0 installed), then you can perform this procedure again, this time removing the MSADC virtual directory.

Note: Before you can perform the IIS Lockdown procedure a second time, you must undo your initial IIS Lockdown configuration. When the system prompts you to do so, click **Yes** to undo your initial configuration. Then proceed to install IIS Lockdown with the removal of the MSADC virtual directory.

To install IIS Lockdown and URLScan

The default installation of IIS Lockdown includes a series of standard server templates that are incompatible with Symposium Web Client. Instead of using the standard configuration, Nortel Networks recommends that you modify one of the standard templates—the Small Business Server 2000 template—to be compatible with Symposium Web Client. The following procedure includes the recommended settings for modifying this template.

Nortel Networks has verified the following configuration to ensure its compatibility with the proper Symposium Web Client application server operation. Therefore, if you choose to alter this recommended configuration to meet specific customer requirements, note that Nortel Networks will not have verified the impact of such a change on the Symposium Web Client application server. Customers who deviate from the recommended IIS Lockdown configuration must test their IIS Lockdown and URLScan configuration with Symposium Web Client in a non-production environment before putting the configuration online.

Note: Before starting this procedure, you must have the Windows 2000 Server CD on hand as the installation wizard may prompt you to insert it in the server.

1 On the application server, open Internet Explorer.

2 In Internet Explorer, navigate to the following Microsoft web page:

http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=DDE9EFC0-BB30-47EB-9A61-FD755D23CDEC

Result: The IIS Lockdown Tool 2.1 page appears.

3 Click **Download**.

Result: The File Download window appears, enabling you to open the installation program immediately, or save the installation file to disk.

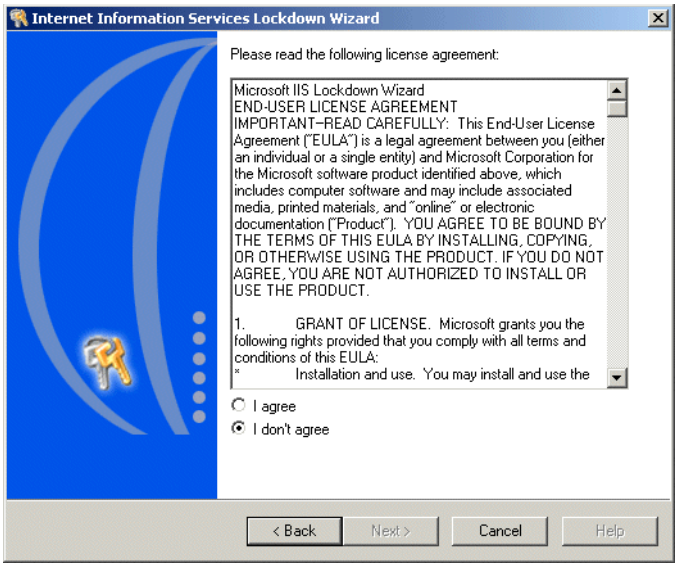
4 Click **Open**.

Note: If you click **Save**, navigate to the folder where you want to save the file, iislokd.exe. Then, install the program by double-clicking this file.

Result: The program extracts files, and then the welcome window appears.

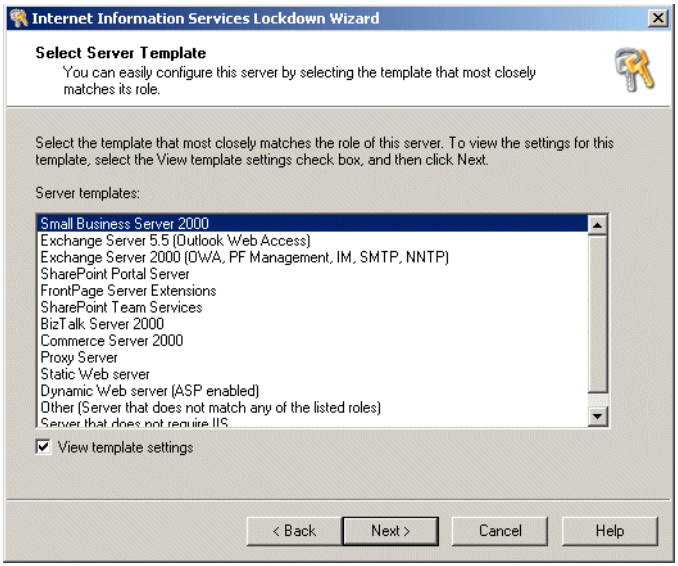
5 Click **Next**.

Result: The license window appears.



6 Click **I agree**, and then click **Next**.

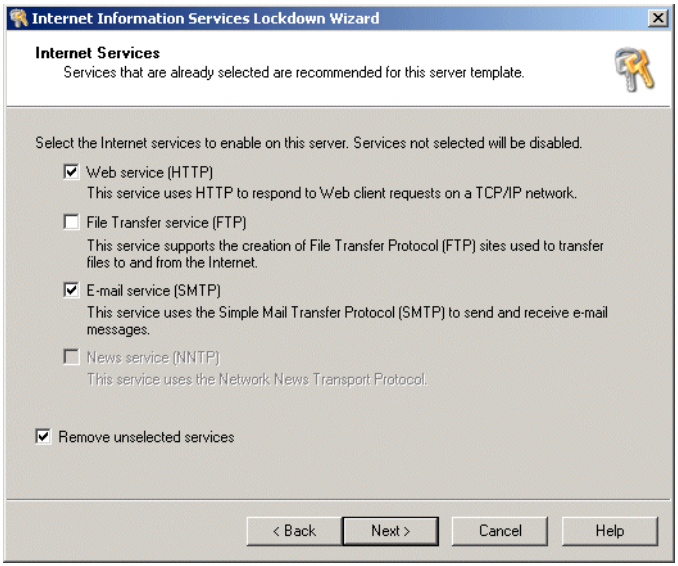
Result: The Select Server Template window appears.



7 From the list of templates, highlight the **Small Business Server 2000** template, and then click the check box beside **View template settings**.

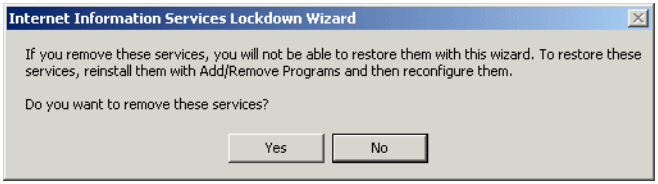
8 Click **Next**.

Result: The Internet Services window appears.



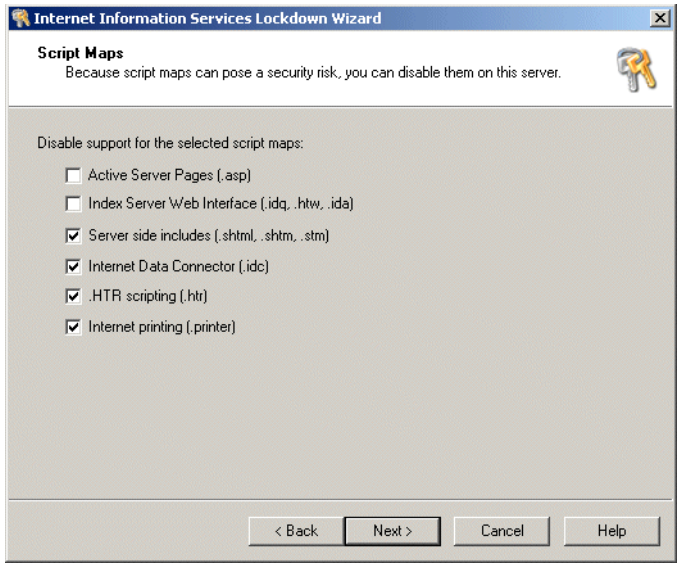
9 Ensure that only **Web service (HTTP)** and **E-mail service (SMTP)** are checked, and then click the check box beside **Remove unselected services**.

Result: A message box appears, asking you to confirm that you want to remove these services.



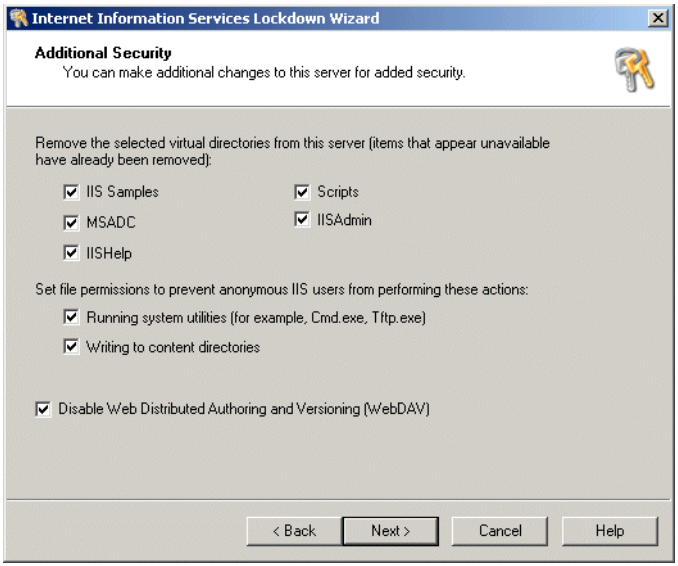
10 Click **Yes**, and then click **Next** in the Internet Services window.

Result: The Script Maps window appears.



11 Ensure there is a check mark beside **Server side includes**, **Internet Data Connector**, **HTR scripting**, and **Internet printing** to disable these items, and then click **Next**.

Result: The Additional Security window appears.



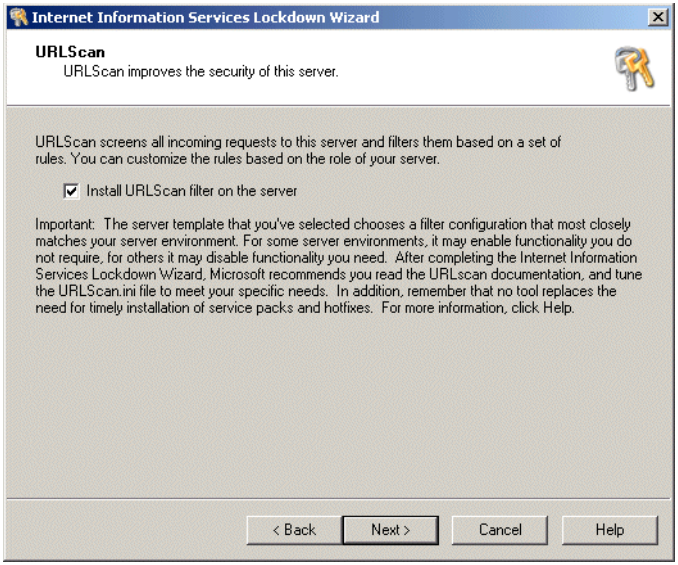
12 Ensure that all virtual directories and file permissions are selected, as shown in the graphic above, and click the check box beside **Disable web Distributed Authoring and Versioning (WebDAV)**. Then click **Next**.

Notes:

- When you select the check box beside Writing to content directories, you prevent the IIS anonymous user from writing to certain .mdb files and export folders, as required by Symposium Web Client. To enable this user to write to the required files and folders, you must perform the procedure “To configure file and folder permissions” on page 220.
- Select the check box beside MSADC *only* if *all* client PCs have client SOAP 3.0 installed, and those running Agent Desktop Displays have been upgraded to Release 4.5 of the software. If any client PCs are running Agent Desktop Displays 4.0, or if they do not have SOAP 3.0 installed yet, then you cannot remove the MSADC virtual directory (because this disables RDS, which is required for Agent Desktop Displays 4.0, and for the upgrade process to SOAP 3.0). In this case, leave the check box beside this directory deselected and continue with

the rest of the procedure. When all client PCs have SOAP 3.0 installed, and those running Agent Desktop Displays have been upgraded to Release 4.5, then you can return to this procedure and select the MSADC virtual directory to remove it.

Result: The URLScan window appears.

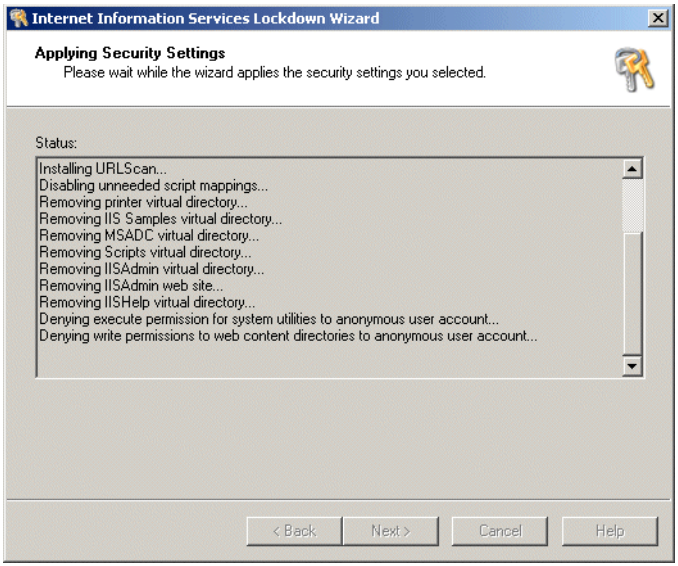


13 Click the check box beside **Install URLScan filter on the server**, and then click **Next**.

Result: The Ready to Apply Settings window appears.

14 Review the settings, and then click **Next** to begin installing IIS Lockdown and URLScan.

Result: The Applying Security Settings window appears, notifying you of the progress of the installation.



Note: The program may prompt you to insert the Windows 2000 CD into the server so it can copy required files. If this message box appears, insert the CD, and then click **OK** to continue the installation.

Result: When the program has finished installing the software, the completing window appears.

15 Click **Finish**.

To configure file and folder permissions

For proper Symposium Web Client functionality, the IIS anonymous user account (IUSR_<*computer_name*>) must have write access to the files and folders shown below.

Note: If you have created a custom account to replace the IUSR_<*computer_name*> account, then you must apply all the file and folder permissions listed in this section to this custom account instead of to the IUSR_<*computer_name*> account.

In the following folder,

C:\Program Files\Nortel Networks\WClient\Apps\Common\icedb

where *C:* is the drive on which you installed Symposium Web Client, the anonymous user must have write access to this file:

- iceLog.mdb

In the following folder,

C:\Program Files\Nortel Networks\WClient\Apps\Reporting\Historical\Data

where *C:* is the drive on which you installed Symposium Web Client, the anonymous user must have write access to these files:

- Nicrpt_dms.mdb
- Nicrpt.mdb
- custform.mdb

In the following folder,

C:\Program Files\Nortel Networks\WClient\Apps\AccessMgmt

where *C:* is the drive on which you installed Symposium Web Client, the anonymous user must have write access to this file:

- counter.xml

In addition to the files listed above, the anonymous user must have write access to the following export folders, where *C:* is the drive on which you installed Symposium Web Client:

- *C:\Program Files\Nortel Networks\WClent\Apps\EmergencyHelp\Exports*
- *C:\Program Files\Nortel Networks\WClent\Apps\Reporting\RealTime\Exports*

The anonymous user must also have write access to the following data folder, where *C:* is the drive on which you installed Symposium Web Client:

- *C:\Program Files\Nortel Networks\WClent\Apps\Reporting\Historical\Data*

When you perform the IIS Lockdown procedure, the system creates an anonymous user group called *_Web Anonymous Users* and designates the IUSR_<*computer name*> user account as a member of this group. To ensure that the IUSR_<*computer name*> user account has write permissions on the files and folders listed above, you must delete the *_Web Anonymous Users* group from the properties dialog for each of the .mdb files shown, and from the properties dialog for each of the folders listed.

1 On the application server, open Windows Explorer and navigate to the following folder,

C:\Program Files\Nortel Networks\WClient\Apps\Common\icedb

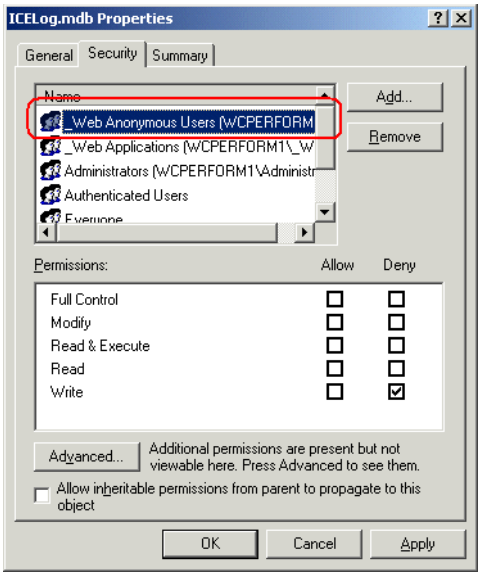
where *C:* is the drive on which you installed Symposium Web Client.

2 In this folder, right-click the file iceLog.mdb, and from the resulting pop-up menu, select **Properties**.

Result: The ICELog.mdb Properties dialog box appears.

3 Click the **Security** tab.

4 In the **Name** box, highlight the _Web Anonymous Users group, and then click **Remove**.



5 Click **OK** to save your changes and close the properties dialog.

6 In Windows Explorer, navigate to the following folder, where *C:* is the drive on which you installed Symposium Web Client:

C:\Program Files\Nortel Networks\WClient\Apps\Reporting\Historical\Data

7 Perform steps 2 to 5 for each of the following files:

- Nicrpt_dms.mdb

- Nicrpt.mdb
- Custform.mdb

8 In Windows Explorer, navigate to the following folder, where *C:* is the drive on which you installed Symposium Web Client:

C:\Program Files\Nortel Networks\WClient\Apps\AccessMgmt

9 Perform steps 2 to 5 for the following file:

- counter.xml

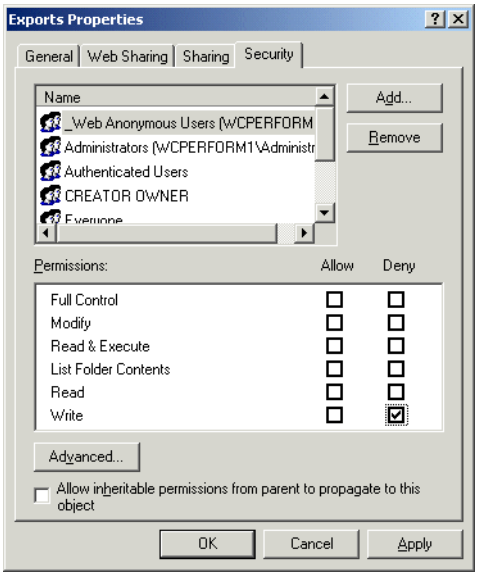
10 To enable write access on the first export folder, in Windows Explorer, navigate to the following folder,

C:\Program Files\Nortel Networks\WClent\Apps\EmergencyHelp\Exports

where *C:*\ is the drive on which you installed Symposium Web Client.

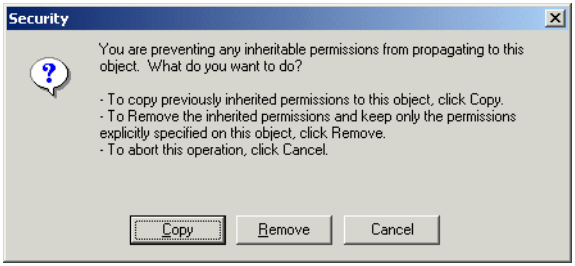
11 Right-click the folder and select Properties from the resulting pop-up menu.

Result: The Exports Properties dialog box appears.



12 Ensure that the check box beside **Allow inheritable permissions from parent to propagate to this folder** is deselected. If it is already

deselected, proceed to step 12. If you have to deselect it, the following message box appears:



13 Click **Copy**.

Result: The system copies the permissions and the properties window reappears.

14 In the properties window, highlight the **_Web Anonymous Users** group, and then click **Remove**.

15 Click **OK** to save your changes and close the properties window.

16 Perform steps 8 to 13 on the following folders:

- *C:\Program Files\Nortel Networks\WClient\Apps\Reporting\RealTime\Exports*
- *C:\Program Files\Nortel Networks\WClient\Apps\Reporting\Historical\Data*

where *C:*\ is the drive on which you installed Symposium Web Client.

To temporarily edit the urlscan.ini file

When you install and configure IIS Lockdown and URLScan according to the procedure above, the configuration does not allow users to download files with the .exe extension from the application server. Since the Symposium Configuration spreadsheets have the .exe extension, administrators cannot download these spreadsheets when the IIS Lockdown and URLScan features are enabled.

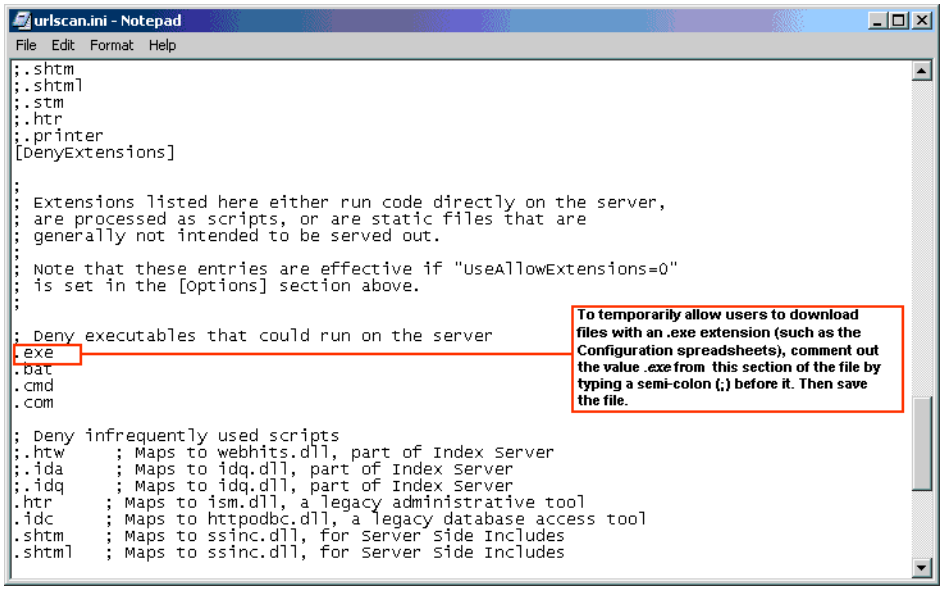
If you need to download a spreadsheet (or another .exe file) while IIS Lockdown is enabled, then you can *temporarily* alter the urlscan.ini file to allow this activity, provided that it conforms to your company's security policy. Once users have finished downloading the required files, edit and save this file again to return the security settings to their default state.

1 On the application server, open the urlscan.ini file with a text editor, such as Notepad. The default location for this file is

C:\WINNT\system32\inetsrv\urlscan\

where *C*: is the drive on which you installed the operating system.

2 In this file, locate the section beginning with *[DenyExtensions]* .



3 Within this section of the file, locate and comment out the value **.exe** (shown in the graphic above) by typing a semi-colon (;) before this value.

4 Save the file.

Result: Users can download the Symposium Configuration spreadsheets (and any other file with an .exe extension) from the application server.

5 When the users have finished downloading the required files, you must return the security settings to normal by opening the urlscan.ini file again and reentering the value .**exe** in the same position.

6 Save the file.

Result: Users can no longer download files with an .exe extension.

To uninstall IIS Lockdown and reconfigure an application server that was installed as the default web site

If you had installed IIS Lockdown before installing Symposium Web Client as the default web site, then you must perform the following steps to recover your application server:

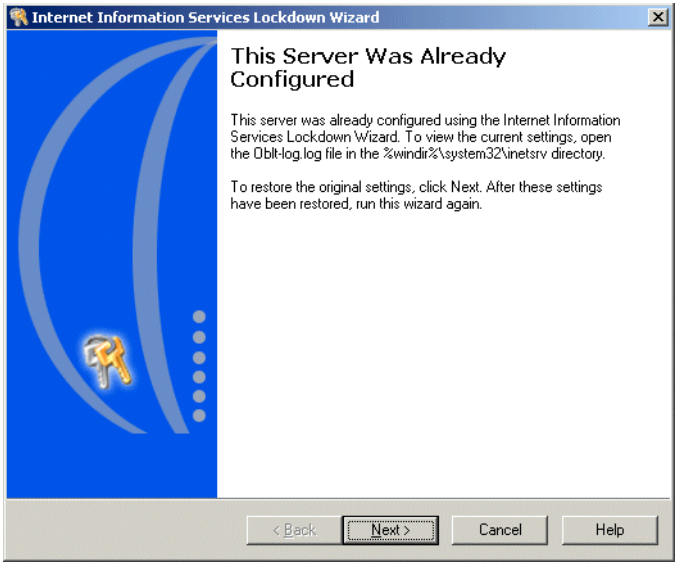
- Uninstall IIS Lockdown by double-clicking the same file that you used to install the software, *iislokd.exe.*
- In IIS, reconfigure the required default paths and virtual directories for proper Symposium Web Client functionality.
- Reinstall IIS Lockdown.

1 On the application server, browse to locate the IIS Lockdown installation file, *iislokd.exe*.

Note: If you have deleted this file since installing IIS Lockdown, you can download it from the Microsoft web site at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/locktool.asp.

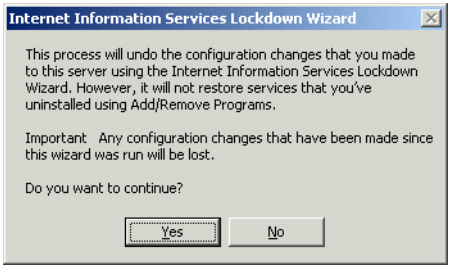
2 Double-click this file.

Result: A window appears, notifying you that you have already performed the IIS Lockdown procedure.



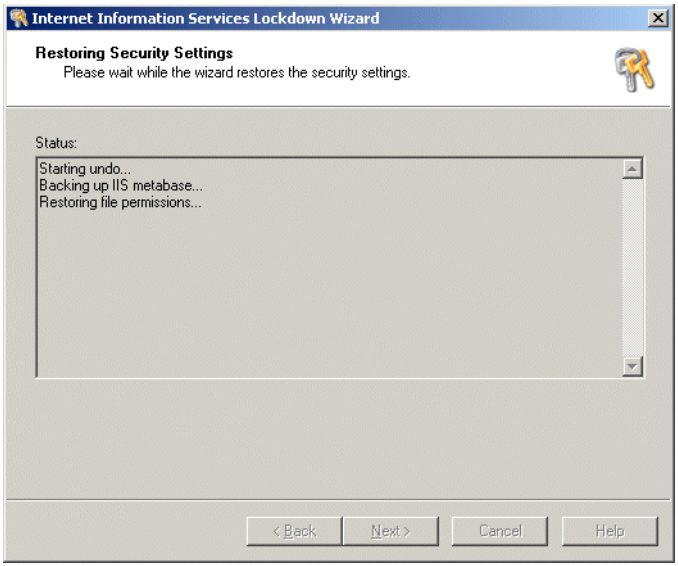
3 To uninstall the software, click **Next**.

Result: A warning box appears.



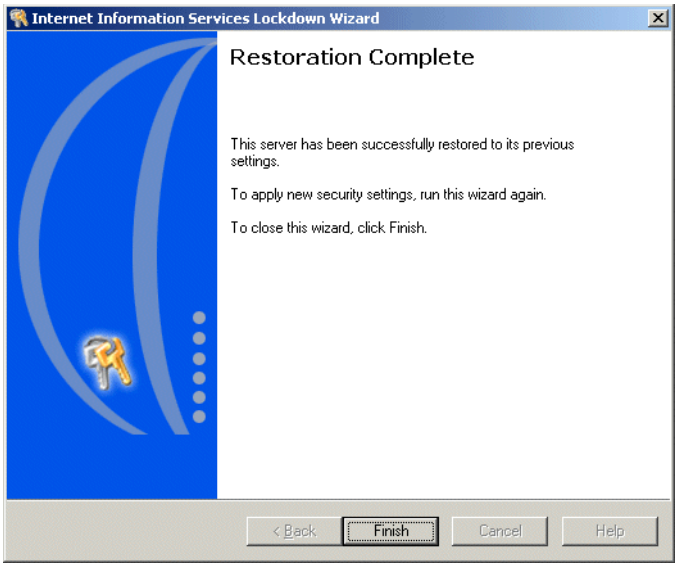
4 Click **Yes**.

Result: The Restoring Security Settings window appears.



5 When the system has restored the settings, click **Next**.

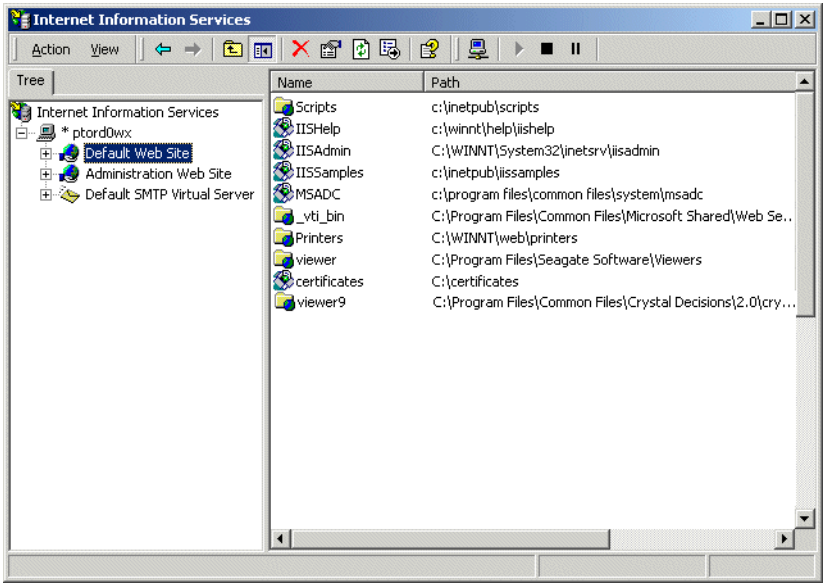
Result: The Restoration Complete window appears.



6 Click **Finish**.

7 Click Start → Programs → Administrative Tools → Internet Services Manager.

Result: The Internet Information Services window appears.



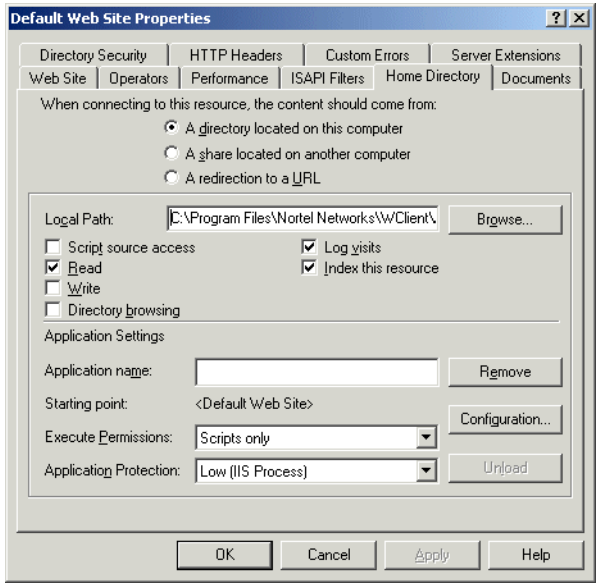
8 In the left pane, double-click the server name.

Result: The name expands to reveal a series of folders.

9 Right-click the Default Web Site heading, and then select **Properties** from the resulting pop-up menu.

Result: The Default Web Site Properties window appears.

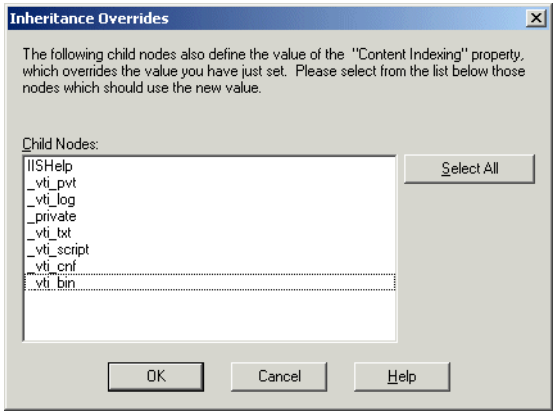
10 Click the **Home Directory** tab.



11 In the **Local Path** box, ensure that the path reads *C:*\Program Files\Nortel Networks\WClient\Apps, where *C:* is the drive on which Symposium Web Client is installed.

12 Click **OK**.

Result: The Inheritance Overrides window may appear. If so, continue with step 13. If this window does not appear, proceed to step 14.



13 Click **Select All**, and then click **OK**.

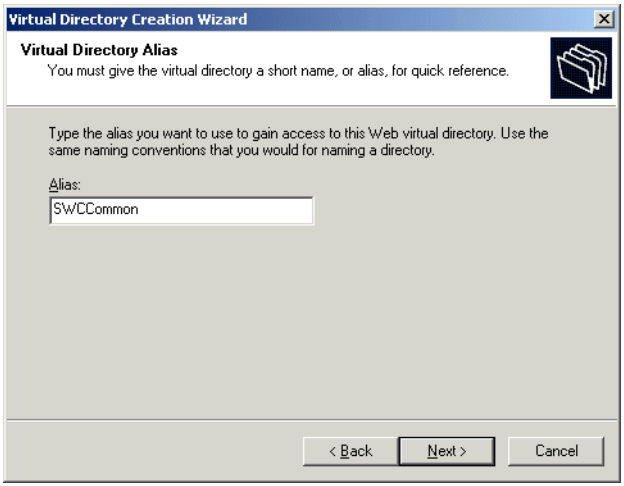
Result: The system saves your changes.

14 In the Internet Information Services window, right-click **Default Web Site**, and then select New → Virtual Directory from the resulting pop-up menu.

Result: The welcome window for the Virtual Directory Creation Wizard appears.

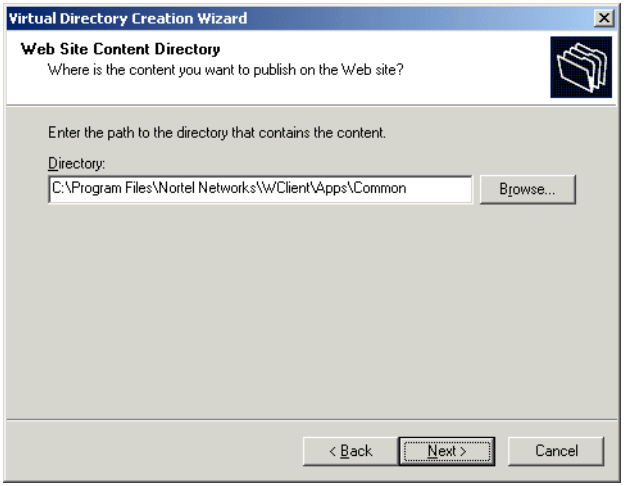
15 Click **Next**.

Result: The Virtual Directory Alias window appears.



16 In the Alias box, type **SWCCommon**, and then click **Next**.

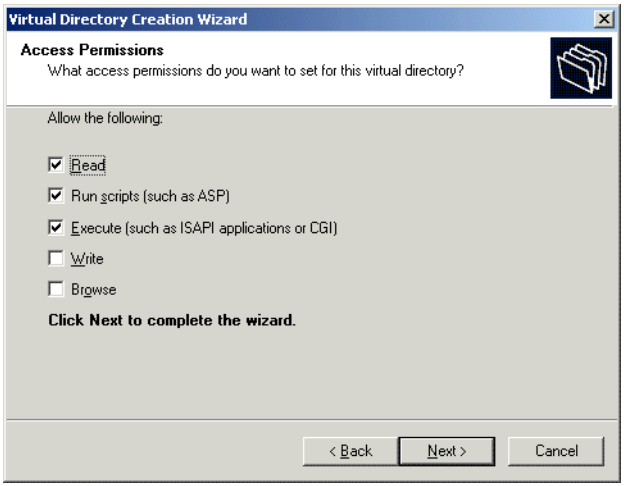
Result: The Web Site Content Directory window appears.



17 Click **Browse** and navigate to the following path: *C:*\Program Files\Nortel Networks\WClient\Apps\Common, where C: is the drive on which you installed Symposium Web Client.

18 Click **Next**.

Result: The Access Permissions window appears.



19 Accept the default values shown in this window, and then click **Next**.

Result: The completion window appears.

20 Click **Finish**.

Result: Your application server is reconfigured. You can now reinstall IIS Lockdown by following the procedure, “To install IIS Lockdown and URLScan” on page 211.

To uninstall IIS Lockdown and reconfigure an application server that was installed as part of an existing site

If you had installed IIS Lockdown before installing Symposium Web Client as part of an existing site, then you must perform the following steps to recover your application server:

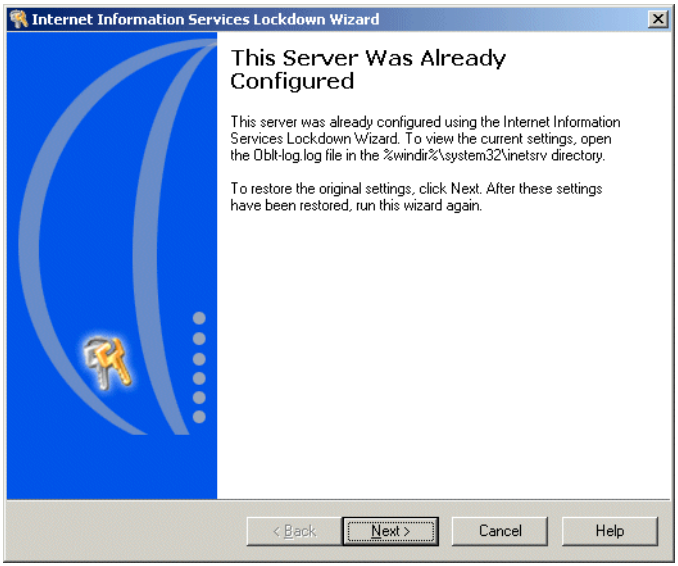
- Uninstall IIS Lockdown by double-clicking the same file that you used to install the software, *iislokd.exe.*
- In IIS, reconfigure the required default paths and virtual directories for proper Symposium Web Client functionality.
- Reinstall IIS Lockdown.

1 On the application server, browse to locate the IIS Lockdown installation file, *iislokd.exe*.

Note: If you have deleted this file since installing IIS Lockdown, you can download it from the Microsoft web site at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/locktool.asp.

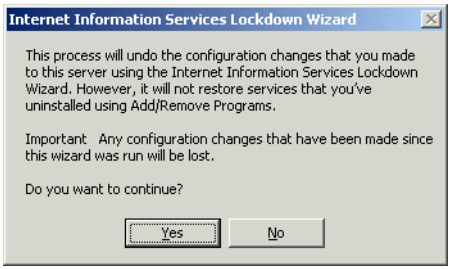
2 Double-click this file.

Result: A window appears, notifying you that you have already performed the IIS Lockdown procedure.



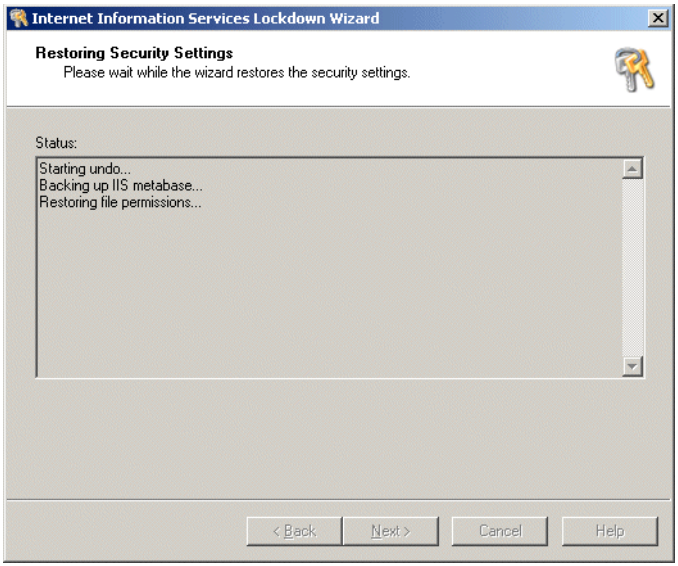
3 To uninstall the software click **Next**.

Result: A warning box appears.



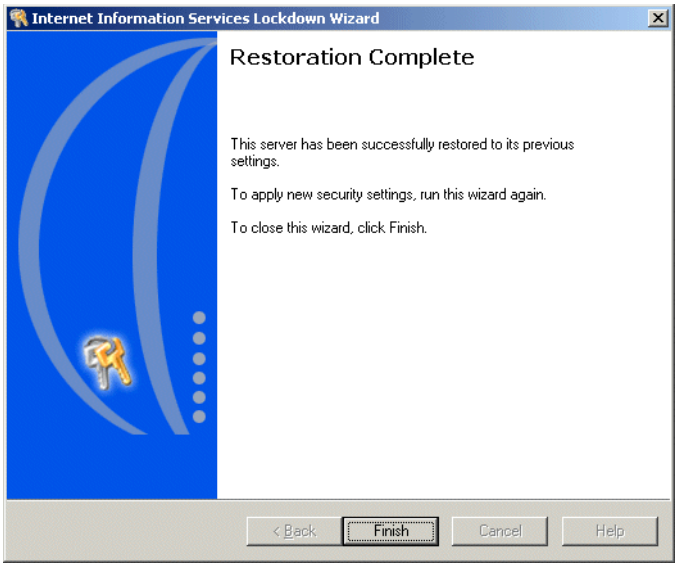
4 Click **Yes**.

Result: The Restoring Security Settings window appears.



5 When the system has restored the settings, click **Next**.

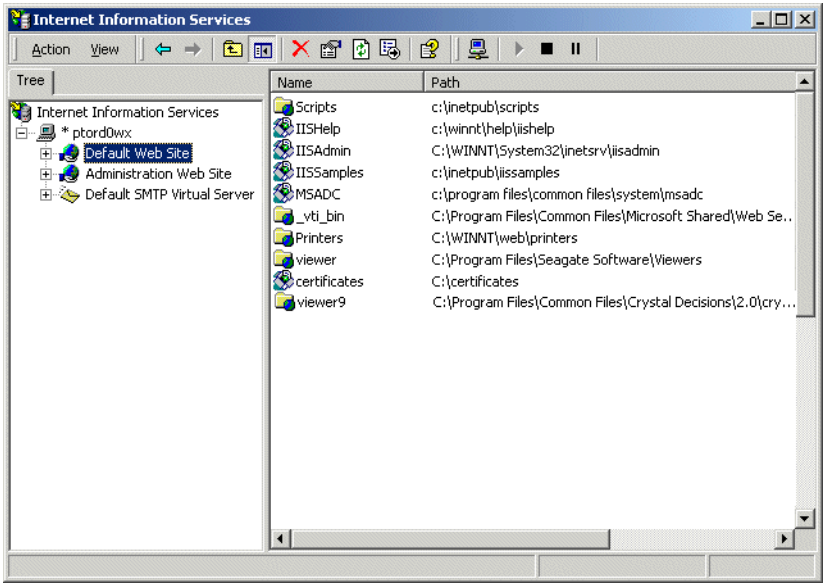
Result: The Restoration Complete window appears.



6 Click **Finish**.

7 Click Start → Programs → Administrative Tools → Internet Services Manager.

Result: The Internet Information Services window appears.

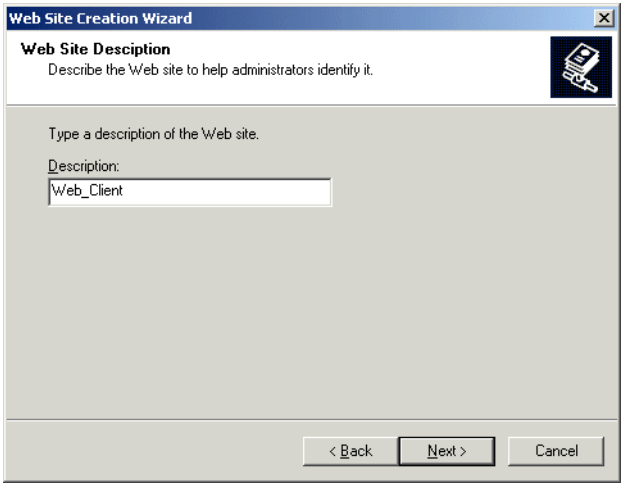


8 Right-click the Default Web Site heading, and then select New → Site from the resulting pop-up menu.

Result: The Web Site Creation Wizard appears.

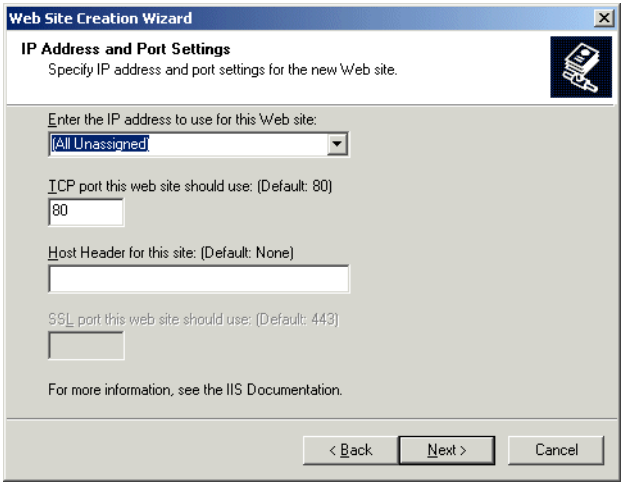
9 Click **Next**.

Result: The Web Site Description window appears.



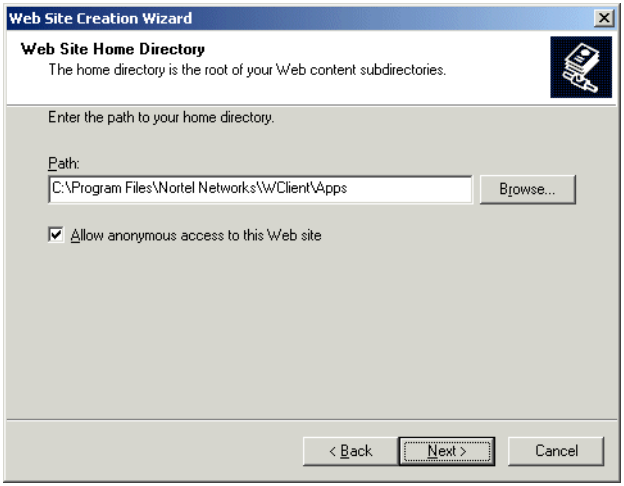
10 In the Description box, type the name of the Symposium Web Client site, and then click **Next**.

Result: The IP Address and Port Settings window appears.



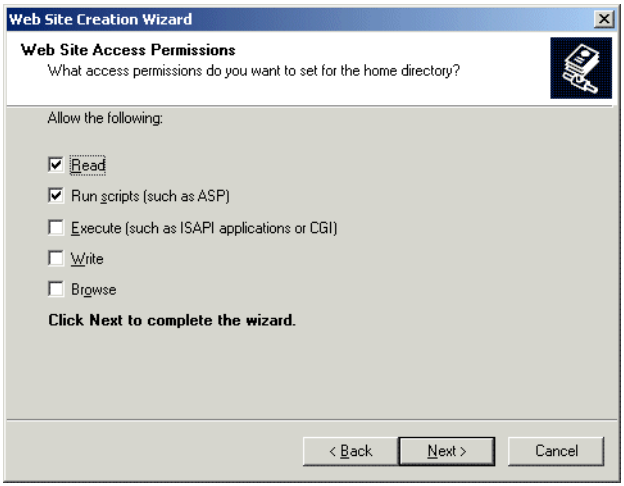
11 Accept the defaults in this window, and then click **Next**.

Result: The Web Site Home Directory window appears.



12 Click **Browse** to navigate to the folder *C:*\Program Files\Nortel Networks\WClient\Apps, where C: is the drive on which you installed Symposium Web Client, and then click **Next**.

Result: The Web Site Access Permissions window appears.



13 Accepts the defaults shown, and then click **Next**.

Result: The completion window appears.

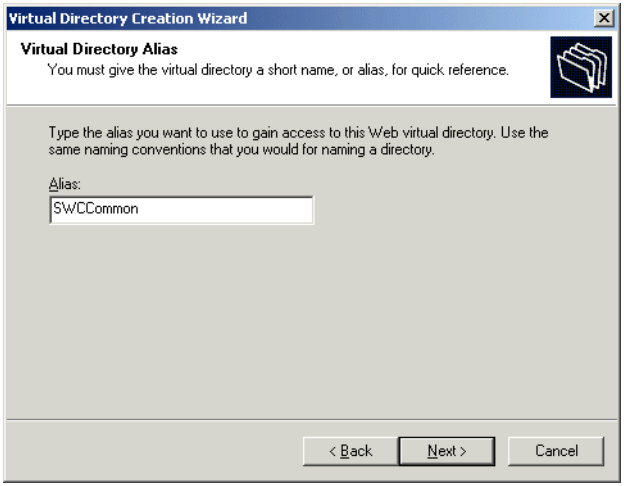
14 Click **Finish**.

15 In the Internet Information Services window, right-click **Default Web Site**, and then select New → Virtual Directory from the resulting pop-up menu.

Result: The Welcome to the Virtual Directory Creation Wizard appears.

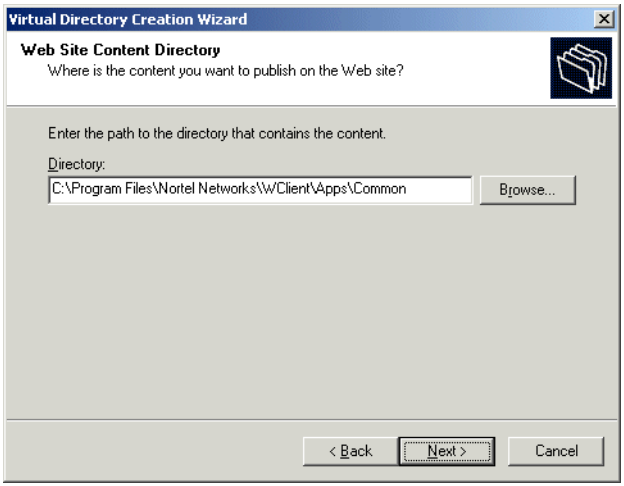
16 Click **Next**.

Result: The Virtual Directory Alias window appears.



17 In the Alias box, type **SWCCommon**, and then click **Next**.

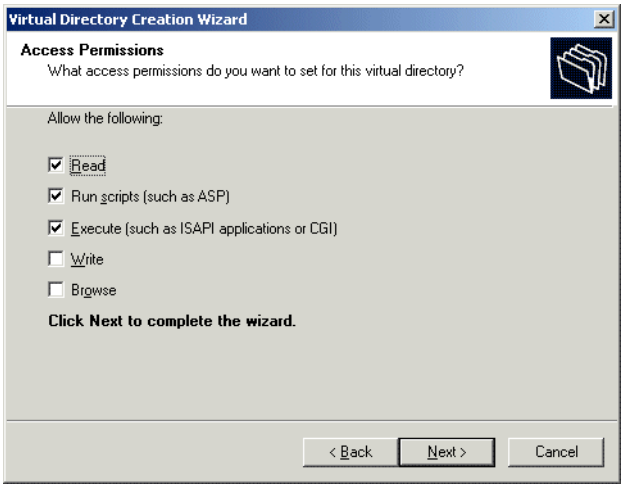
Result: The Web Site Content Directory window appears.



18 Click **Browse** and navigate to the following path: *C:*\Program Files\Nortel Networks\WClient\Apps\Common, where C: is the drive on which you installed Symposium Web Client.

19 Click **Next**.

Result: The Access Permissions window appears.



20 Accept the defaults shown in this window, and then click **Next**.

Result: The completion window appears.

21 Click **Finish**.

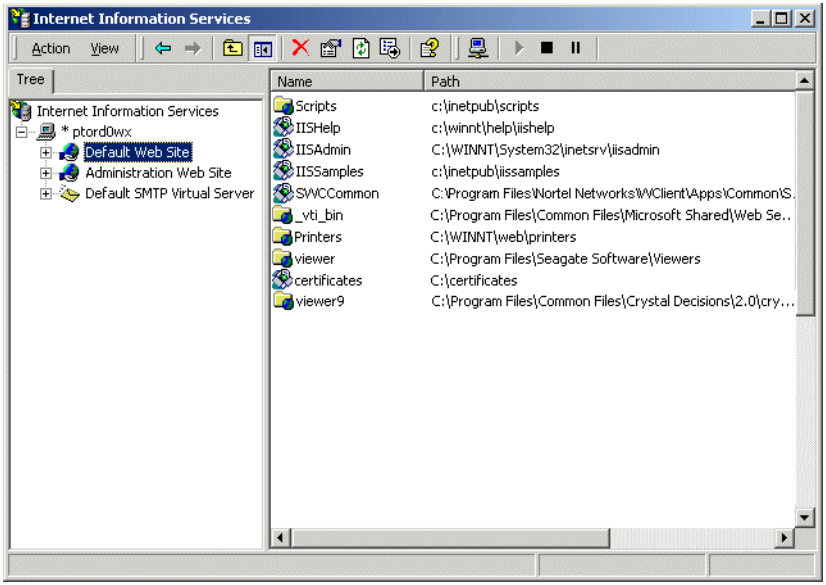
Result: Your application server is reconfigured. You can now reinstall IIS Lockdown by following, “To install IIS Lockdown and URLScan” on page 211.

To reenable Remote Data Service

If you have disabled Remote Data Service (RDS) by removing the MSADC virtual directory in the IIS Lockdown procedure, and now you want to use Agent Desktop Displays 4.0 to connect to Symposium Web Client 4.5, then you must reenable RDS by adding this folder back in IIS.

1 Click Start → Programs → Administrative Tools → Internet Services Manager.

Result: The Internet Information Services window appears.

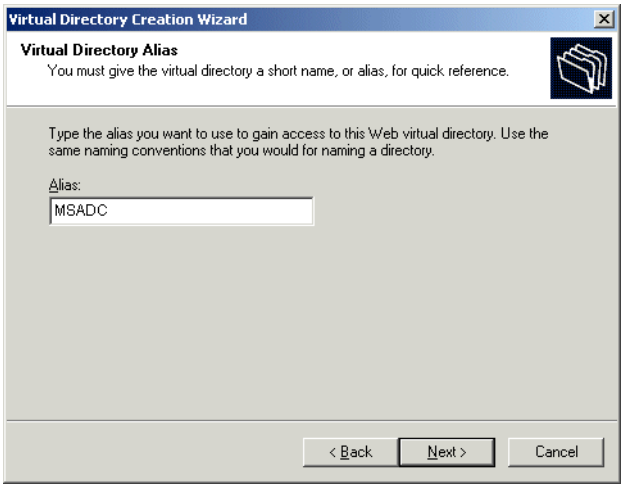


2 In the Internet Information Services window, right-click **Default Web Site**, and then select New → Virtual Directory from the resulting pop-up menu.

Result: The welcome window for the VIrtual Directory Creation Wizard appears.

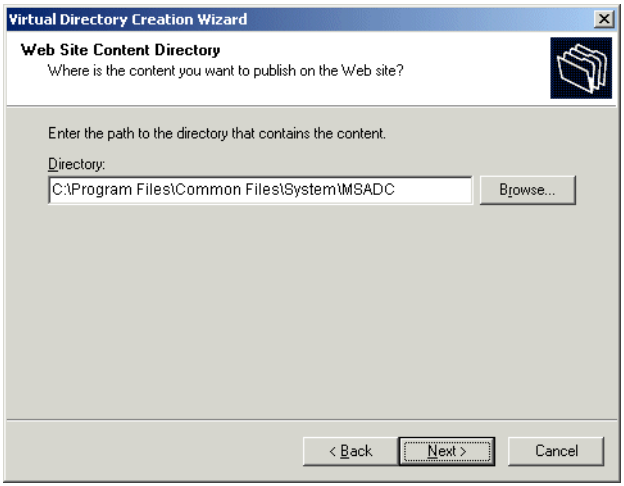
3 Click **Next**.

Result: The Virtual Directory Alias window appears.



4 In the Alias box, type **MSADC**, and then click **Next**.

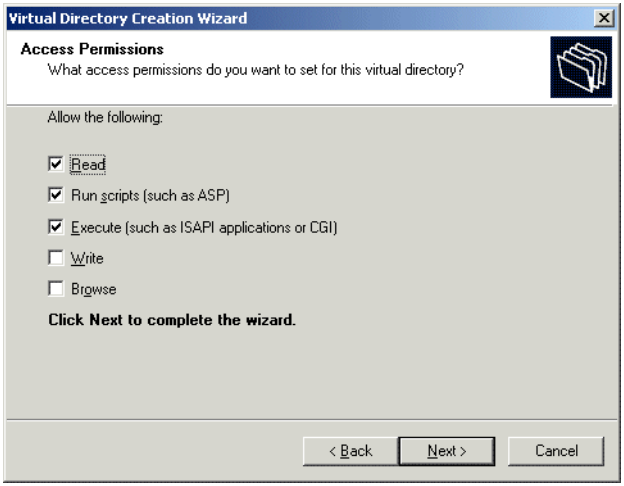
Result: The Web Site Content Directory window appears.



5 Click **Browse** and navigate to the following path: *C:*\Program Files\Common Files\System, where C: is the drive on which you installed Symposium Web Client.

6 Click **Next**.

Result: The Access Permissions window appears.



7 Ensure that the values **Read**, **Run Scripts**, and **Execute** are selected, and then click **Next**.

Result: The completion window appears.

8 Click **Finish**.

Result: The system creates the MSADC virtual directory in the path you indicated and reenables RDS.

Changing the default anonymous Internet Guest account

Introduction

Symposium Web Client uses the anonymous Internet Guest account for clients accessing the Symposium Web Client application server. This section explains the characteristics of the default Windows 2000 account used for anonymous access, and provides steps that you can perform if you want to create and configure a new account for anonymous access.

Notes:

- The procedure in this section also applies to Windows 2000 Advanced Server.
- You do not have to change the default anonymous Internet Guest account; this is an optional procedure that you can perform if you think that using this account poses a security risk to your organization.

ATTENTION

If you change or create a new IUSR_<*computer name*> user account in the following procedure, then you must use this new account throughout the procedure on removing the Everyone group wherever it lists the IUSR_<*computer name*> user account. For more information, see “Removing the Everyone group from the application server” on page 200.

Characteristics of the default anonymous Internet Guest account

When you install IIS, by default the system configures anonymous access as the directory security for a virtual directory on IIS. The system then uses the default Windows 2000 Internet Guest account, IUSR_*<computer name>*, to grant access to this virtual directory without requesting the user to enter valid user account details.

The Internet Guest account has two notable characteristics:

- It has Log on Locally permissions.
- It is a member of both the Guest and Domain Users groups in Windows 2000.

You must carefully review the file permissions that you give to both the Guest and Domain Users groups to ensure that the permissions are appropriate for your anonymous users.

Since the name of the Internet Guest account is always IUSR_*<computer_name>*, it is known to hackers and can therefore be seen as a security risk. If you foresee using this account as a security risk, Nortel Networks recommends that you designate a different account to use for anonymous access, thereby enabling you to be more specific with your NTFS file permissions.

Note: The Internet Guest account is persistent in IIS, so if you delete or remove the account, the system recreates it the next time the server restarts. Nortel Networks recommends, therefore, that you disable the account to prevent its recreation.

To change the default anonymous Internet Guest account, you must perform the following three procedures:

1. Disable the default anonymous access account, IUSR_*<computer_name>*.
2. Create a new anonymous access user account with the required privileges (or, to save time, copy the existing user account and change its properties).
3. Designate the new account as the account used for anonymous access.

To disable the default anonymous access user account

1 Click Start → Programs → Administrative Tools → Active Directory Users and Computers.

Result: The Active Directory Users and Computers window appears.

2 In the tree in the left pane, double-click the <*computer name*> heading.

Result: The heading expands to reveal a series of folders.

3 Click the Users folder.

Result: The list of users configured in Active Directory appears in the right pane.

4 Right-click the IUSR_<*computer name*> user, and then select **Disable Account** from the resulting pop-up menu.

Result: A message box appears informing you that the account has been disabled.

5 Click **OK**.

To create a new anonymous access user account

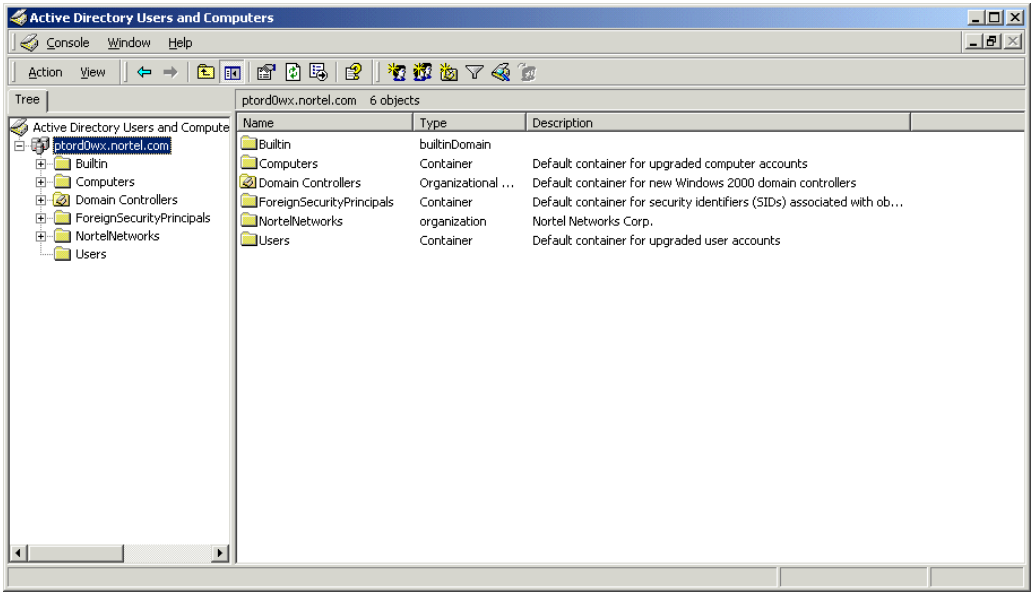
This procedure outlines how to create a new anonymous access user account from scratch. Alternately, to save time, you can copy the existing IUSR_<*computer name*> account, and then change its properties to suit your needs instead of creating a new account. For details on copying the existing account, see “To copy an existing anonymous access user account” on page 255.

1 Click Start → Programs → Administrative Tools → Active Directory Users and Computers.

Result: The Active Directory Users and Computers window appears.

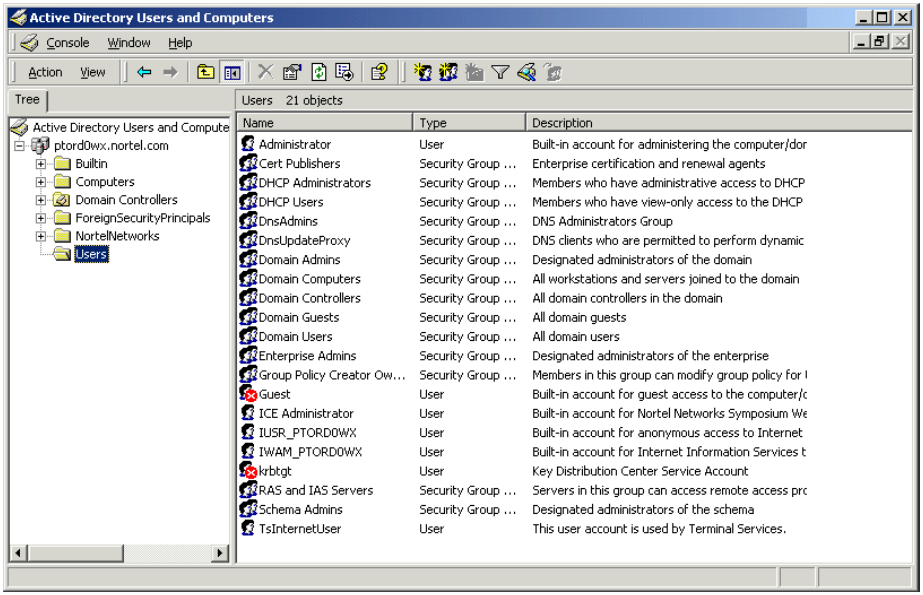
2 In the tree in the left pane, double-click the <*computer name*> heading.

Result: The heading expands to reveal a series of folders.



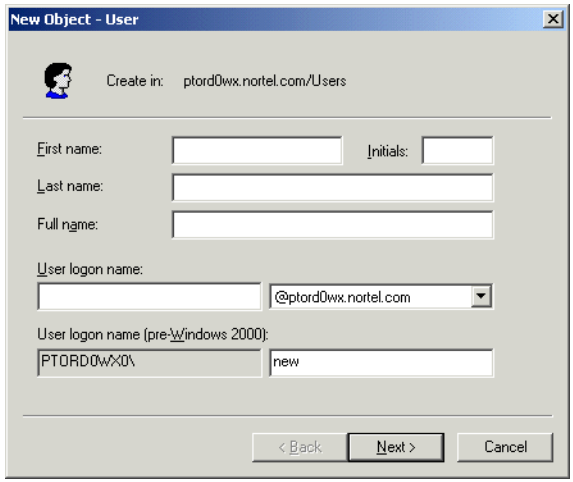
3 Click the Users folder.

Result: The list of users configured in Active Directory appears in the right pane.



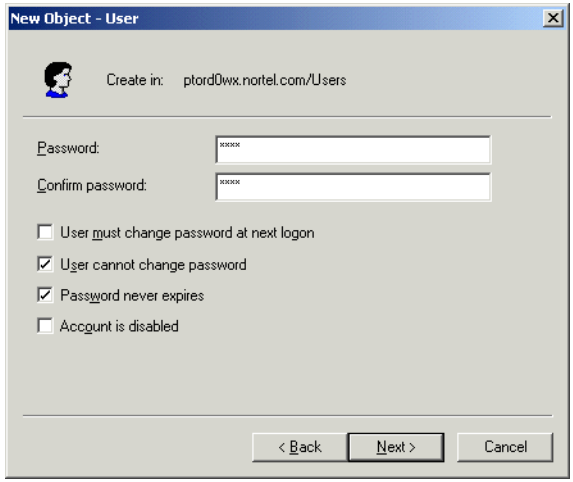
4 Click Action → New → User.

Result: The New Object - User window appears.



5 Type the name and user logon name of the new user, and then click **Next**.

Result: A second New Object - User window appears.

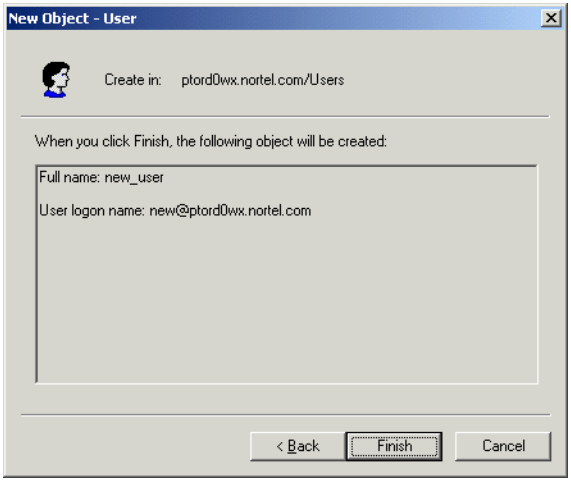


6 In the Password box, type the password for the user account.

7 Click to place a check mark beside **User cannot change password** and **Password never expires**.

8 Click **Next**.

Result: The final New Object - User window appears, listing the new user's details.



9 If you are satisfied with the user's details, click **Finish**.

Note: To change any of the user's details, click **Back**.

10 The system creates the new user and the Active Directory Users and Computers window reappears. The new user account appears in the list of Active Directory users.

11 To add the new user to the Guests and Domain Users groups, right-click the user name and select **Properties** from the pop-up menu.

Result: The <*user name*> Properties window appears.

12 Click the **Member Of** tab.

13 Below the Member of box, click **Add**.

Result: The Select Groups window appears.

14 Select the name **Guests**.

15 Click **Add**.

Result: The new user is added to the Guests group.

16 Select the name **Domain Users**.

17 Click **Add**.

Result: The new user is added to the Domain Users group.

18 Click **OK** twice to save your changes and return to the Active Directory Users and Computers window.

19 Continue with the procedure “To configure the new user account for anonymous access” on page 258.

To copy an existing anonymous access user account

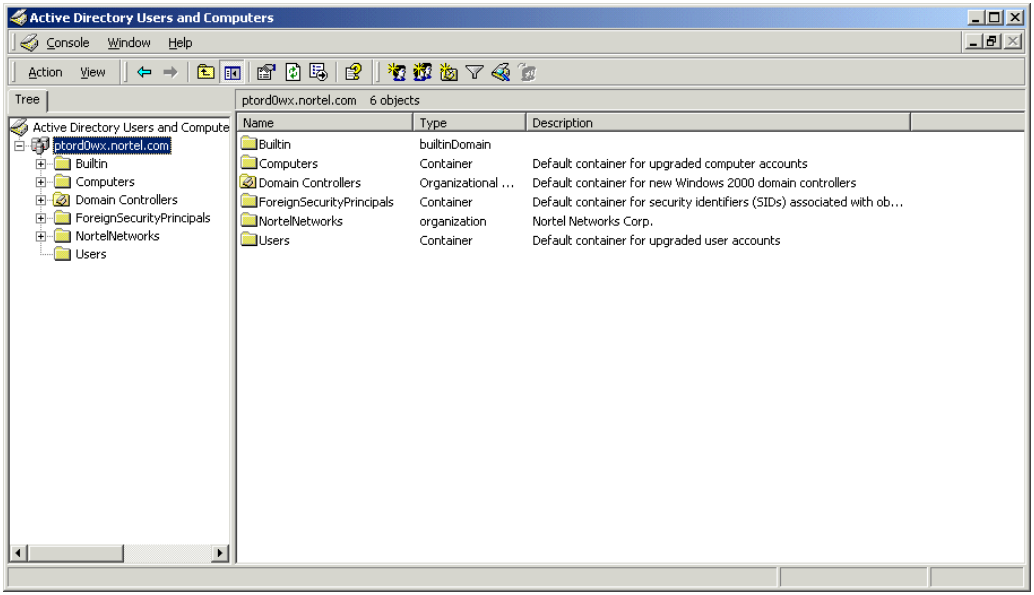
To save time, instead of creating a new anonymous Internet guest account from scratch, you can perform the following procedure to copy the existing anonymous access user account and change its properties to suit your needs. The copied user account inherits some of the original account’s properties, meaning you do not have to configure them again (for example, it is automatically part of the Domain Users and Guests groups).

1 Click Start → Programs → Administrative Tools → Active Directory Users and Computers.

Result: The Active Directory Users and Computers window appears.

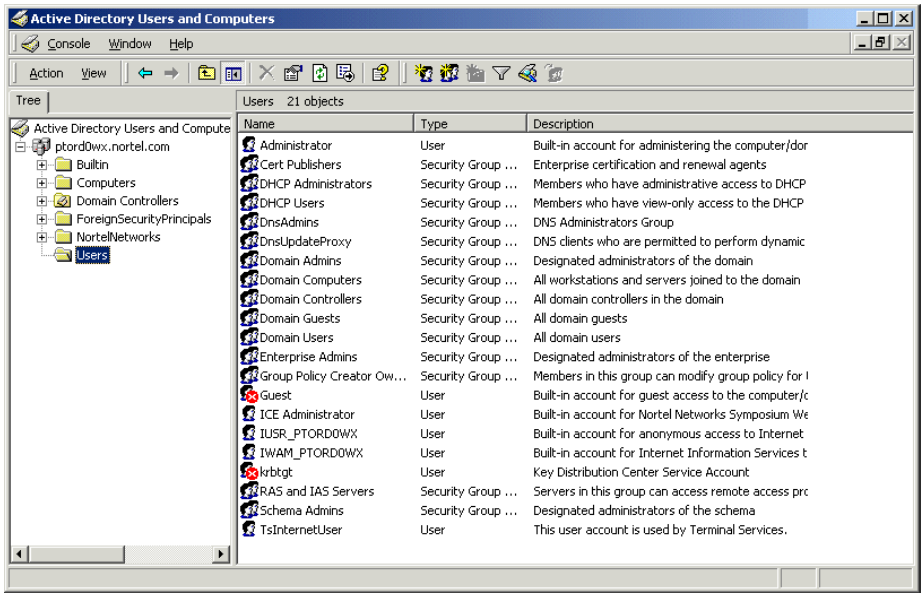
2 In the tree in the left pane, double-click the <*computer name*> heading.

Result: The heading expands to reveal a series of folders.



3 Click the Users folder.

Result: The list of users configured in Active Directory appears in the right pane.



4 From the list of users in the right pane, select and right-click the IUSR_<*computer name*> user.

5 From the resulting pop-up menu, select **Copy**.

Result: The Copy Object - User window appears.

6 Type the name and user logon name of the new user, and then click **Next**.

Result: A second Copy Object - User window appears.

7 In the Password box, type the password for the user account.

8 Click to place a check mark beside **User cannot change password** and **Password never expires**.

9 Click **Next**.

Result: The final Copy Object - User window appears, listing the copied user's details.

10 If you are satisfied with the user's details, click **Finish**.

Note: To change any of the user's details, click **Back**.

11 The system creates the new user and the Active Directory Users and Computers window reappears. The copied user account appears in the list of Active Directory users. This user account inherits some properties from

the original anonymous access user account (for example, it is already a member of the Domain Users and Guests groups.)

12 Continue with “To configure the new user account for anonymous access” below.

To configure the new user account for anonymous access

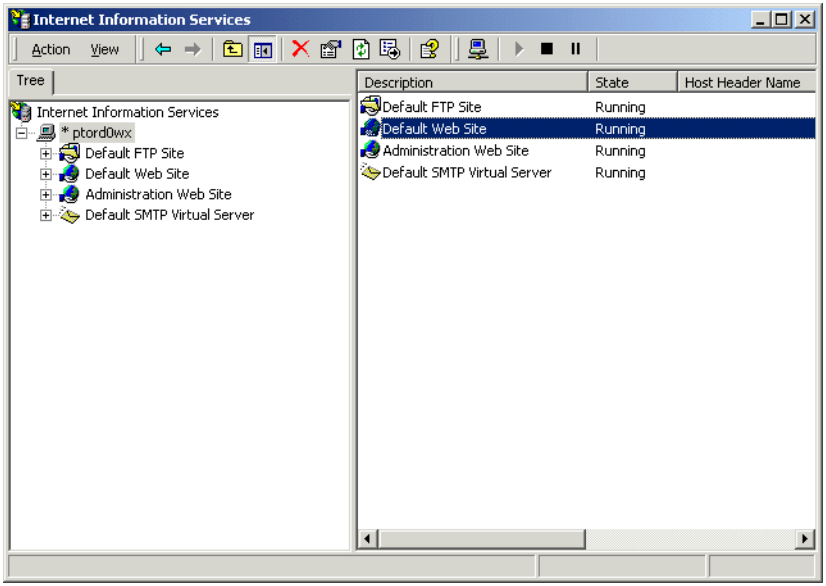
After you have created the new user account (or copied the existing anonymous access user account) in the above procedures, you must configure it for anonymous access.

1 Click Start → Programs → Administrative Tools → Internet Services Manager.

Result: The Internet Information Services window appears.

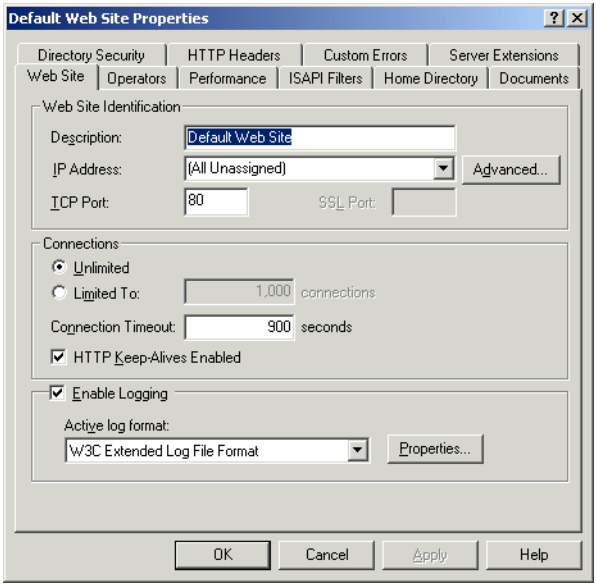
2 In the left pane, double-click the computer name heading.

Result: The heading expands to reveal a series of folders.

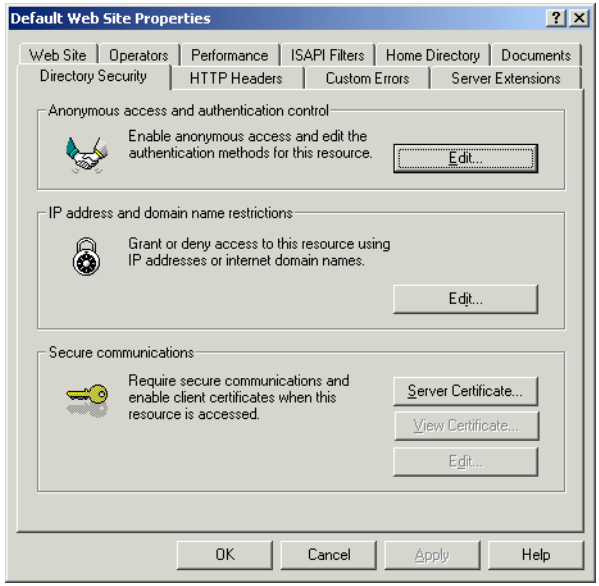


3 Right-click **Default Web Site**, and then click **Properties** from the resulting pop-up menu.

Result: The Default Web Site Properties window appears.

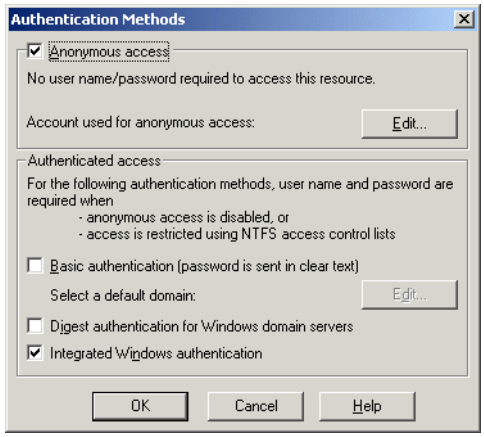


4 Click the Directory Security tab.



5 Under the Anonymous access and authentication control heading, click **Edit**.

Result: The Authentication window appears.



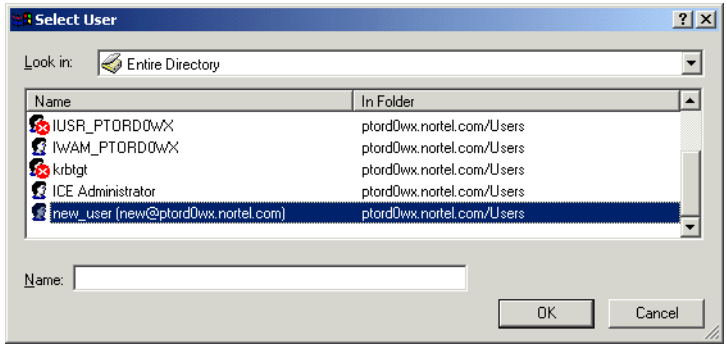
6 Ensure there is a check mark beside Anonymous access.

7 Beside Account used for anonymous access, click **Edit**.

Result: The Anonymous User Account window appears.

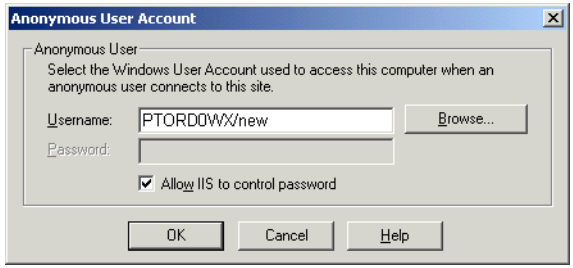
8 Click **Browse** to locate the new user that you created in the previous procedure.

Result: The Select User window appears.



9 Select the new user and then click **OK**.

Result: The Anonymous User Account window reappears listing the new user account in the Username box.



10 Ensure that **Allow IIS to control password** is checked.

11 Click **OK** to return to the Authentication Methods window.

12 Close the Authentication Methods window.

Disabling the parent path in IIS

Introduction

When parent paths are enabled for the Symposium Web Client web site, ASP pages can use relative paths (using the ".." syntax) to navigate to the parent directory of the current directory. This setup can potentially pose a security risk in that it enables hackers to navigate to the parent directory without knowing the directory name.

Once inside the parent directory, if access permissions are not set up correctly, hackers could copy and execute files from it, causing a disruption in Symposium Web Client functionality. For example, if you have set up limited access on the Web Client virtual directory, but you have left execute and write access permissions on the parent directory, then hackers could copy a script or an executable to the parent directory and execute it from there.

Note: You do not have to disable the parent paths in IIS; this is an optional procedure that you can perform if you think that enabling this feature poses a security risk to your organization.

To disable the parent path in IIS

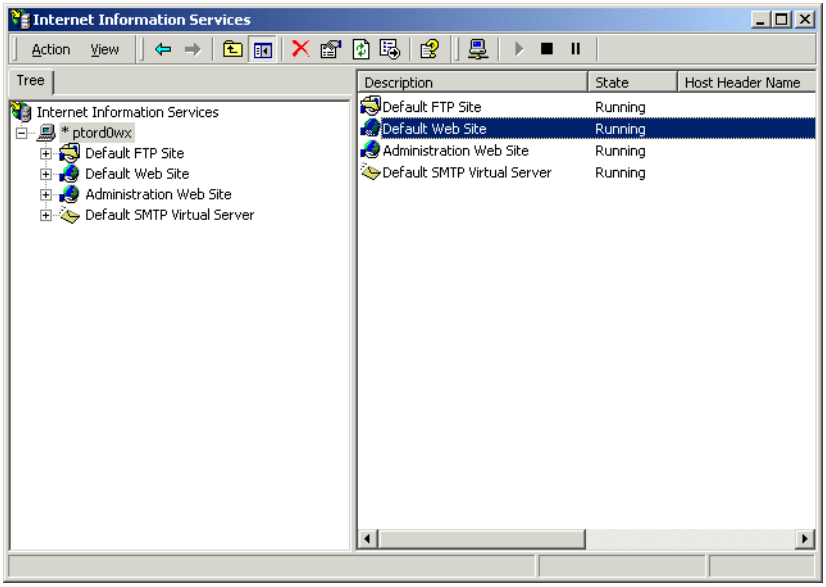
To disable the parent path feature, you need to update the properties for the Symposium Web Client web site.

1 Click Start → Programs → Administrative Tools → Internet Services Manager.

Result: The Internet Information Services window appears.

2 In the left pane, double-click the computer name heading.

Result: The heading expands to reveal a series of folders.



3 In the left pane, right-click the Symposium Web Client web site (this can be either the default web site, or another web site), and then choose **Properties** from the resulting pop-up menu.

Result: The <*web site name*> Properties window appears.

4 Click the Home Directory tab.

5 Under the Application Settings heading, click **Configuration**.

Result: The Application Configuration window appears.

6 Click the App Options tab.

7 Deselect the check mark in the **Enable parent paths** check box.

8 Click **OK**.

Result: The Inheritance Overrides window appears, listing the child nodes that are affected by this change (if applicable).

Note: The Inheritance Overrides window appears only if your IIS administrator has set up IISAdmin and IISHelp as virtual directories on the Symposium Web Client web site. If these virtual directories do not exist, then this window does not appear.

9 Select the nodes that you want to change, and then click **OK**.

10 Click **OK** to save your changes and return to the <*web site name*> Properties window.

11 Click **OK** to close the window.

Enabling Secure Sockets Layer on the application server

Introduction

Secure Sockets Layer (SSL) is the industry standard for secure network communications. SSL uses encryption that cannot be deciphered without a key between the client computer and the server.

SSL is best used on private data that is sent between the client and server (for example, authentication credentials, credit card numbers, and so on). Since SSL uses complex encryption, it requires considerable processor resources, and, as a result, it takes much longer to send and retrieve data from an SSL-enabled server. Therefore, only web pages (ASP pages) that send and receive sensitive information should have SSL enabled.

Note: You do not have to enable SSL on the application server; this is an optional procedure that you can perform if you think that leaving this feature disabled poses a security risk to your organization.

To enable SSL on the application server, you must perform the following two procedures:

1. Obtain and install a digital Web Server Certificate for the Symposium Web Client IIS default web site.
2. Enable SSL on specific Symposium Web Client files (listed below).

Obtaining and installing a digital Web Server Certificate

Since obtaining and installing a digital Web Server Certificate is a standard Microsoft procedure, this guide does not include the step-by-step details. For further information about certificates and installation instructions, see the Microsoft web site at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/iis/maintain/featusability/c06iis.asp.

In IIS, you install the certificate on the Default Web Site (where the Symposium Web Client virtual directories are installed) by using the Web Server Certificate Wizard to request a new certificate from an online Certification Authority (CA), such as VeriSign. When you run the wizard, you can send the request online or save the request file to disk and send it to the CA later. When you receive a response from the CA, you can start the wizard again to complete the certificate installation.

Web sites containing further information on digital certificates

At the time of publication, you can consult the following Microsoft web pages for further information on SSL:

- For general information on SSL, see http://support.microsoft.com/default.aspx?scid=kb;EN-US;q245152.
- For more information on obtaining a server certificate, see http://support.microsoft.com/default.aspx?scid=kb;en-us;Q142849.
- For more information on enabling SSL on Windows 2000, see http://msdn.microsoft.com/library/default.asp?url=/library/en-us/sqlce/connectivity_1s4w.asp.

Tasks for which you can enable SSL on the application server

You can only enable SSL for the following Symposium Web Client tasks, not for the entire web site:

- logging on to the application server
- changing the logon password

See the following procedure for a list of the specific Symposium Web Client files on which you enable SSL.

To enable SSL on the application server

Once you have obtained and installed the certificate on the Symposium Web Client default web site, enable SSL on the following files:

- In the Default Web Site directory:
  - Authenticate.asp

- ChgPasswd.asp
- Default.asp
- PwdMain.asp
- PwdSave.asp

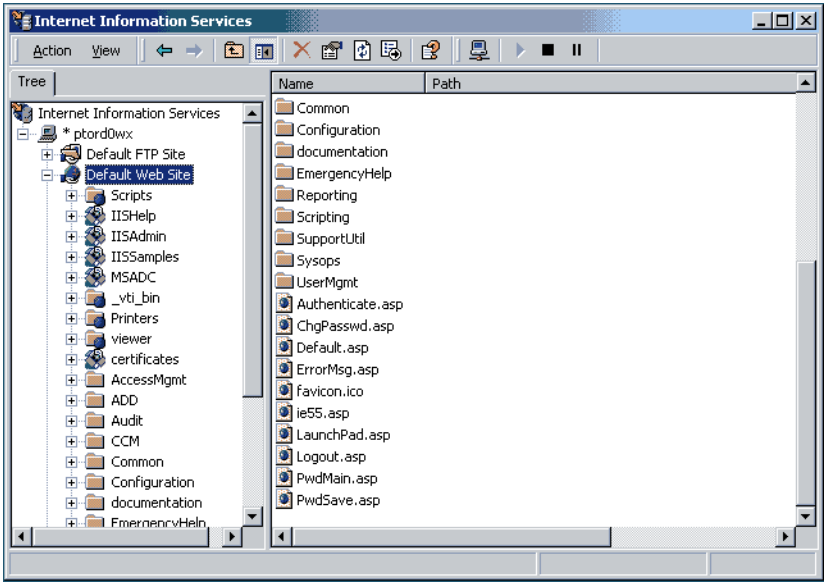
1 Click Start → Programs → Administrative Tools → Internet Services Manager.

Result: The Internet Information Services window appears.

2 In the left pane, double-click the Default Web Site heading.

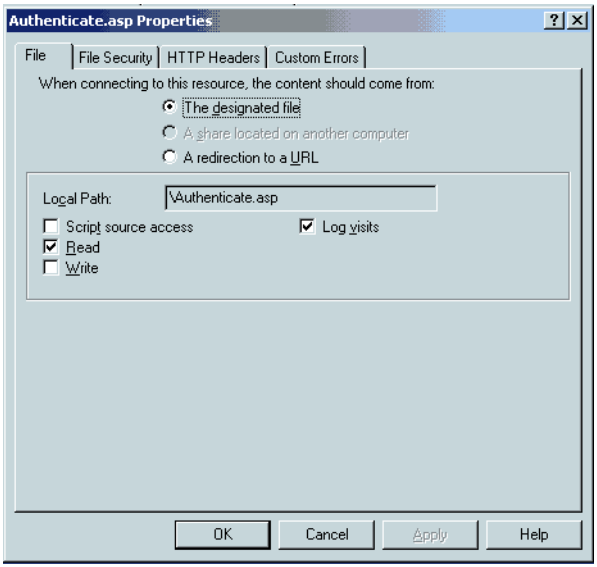
Result: The heading expands to reveal a series of folders.

3 In the right pane, scroll down to the bottom to locate the series of .asp files listed under the Default Web Site heading above.

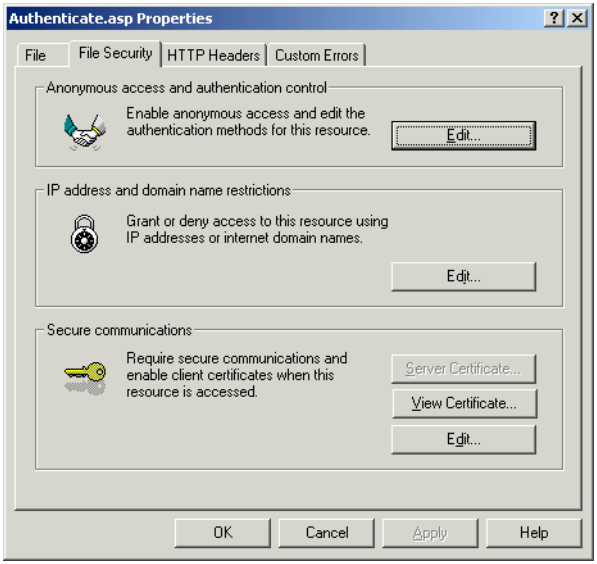


4 Starting with Authenticate.asp, right-click the file and select **Properties**.

Result: The *<file name>* Properties window appears.

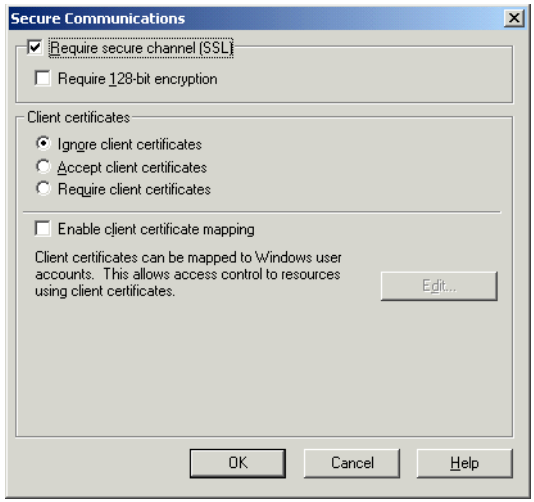


5 Click the **File Security** tab.



6 Under the Secure Communications heading, click **Edit**.

Result: The Secure Communications window appears.



7 Click to select the check box beside **Require secure channel (SSL)**.

8 Click **OK**.

9 Perform steps 4 to 8 for each of the files listed at the beginning of this procedure. When you are finished, close the Internet Information Services window.

10 After you have enabled SSL for each of the files, in an Internet Explorer browser window, click Tools → Internet Options.

11 Click the **Advanced** tab.

12 Scroll down to the bottom of the Settings box until you see the Security section.

13 Select the **Warn if changing between secure and not secure mode** option.

Note: If you do not want to receive a warning message each time you log on to Symposium Web Client, then you can leave this option deselected.

14 Click **OK**.

Configuring Terminal Services in a secure environment

Introduction

The default installation of Terminal Services includes the TsInternetUser account. When you configure Terminal Services for Symposium Web Client, you can use this account for all users who access the Scripting component in Symposium Web Client by configuring the account in Active Directory, and then granting this user account certain access rights and permissions to the Scripting component on the application server.

This default configuration enables all users who have access to the Terminal Services Client to log on to Terminal Services on the application server without entering a user ID or password, which some organizations may consider a security risk.

Alternately, you can create one or more Active Directory accounts of your choice and then configure them so that users must enter either the password and user ID, or just the password *each time* they launch the Scripting component in Symposium Web Client. This section provides instructions for configuring this type of account. If you want to create more than one account (for example, if you want each Scripting user to have their own account), then you must perform all the steps in this section for each account that you create.

Note: If you create a more secure environment by creating and using the Active Directory account of your choice, then Nortel Networks recommends that you disable the TsInternetUser account. For more information, see “To disable the TsInternetUser account” on page 285.

Configuring Terminal Services in a secure environment involves the following main steps:

- create the new user account in Active Directory
- add the new user account to the domain controller local security policy
- grant the new user account the required permissions on selected folders on the application server

- configure the new user account in Terminal Services
- disable the TsInternetUser account (recommended)

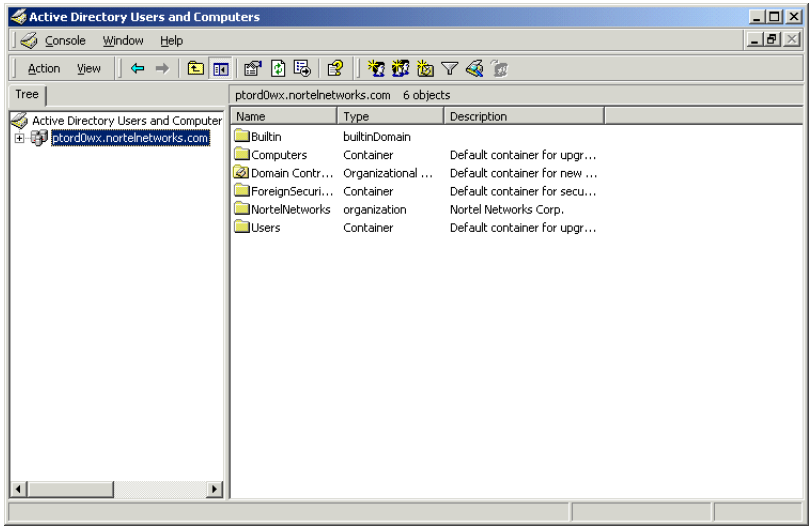
To create a new user account in Active Directory

You can use this procedure to create one or more accounts of your choice to be used when logging on to the Scripting component.

Note: In this procedure, the sample user account *swcts* is created. Wherever you see this value, replace it with the user account of your choice.

1 Click Start → Programs → Administrative Tools → Active Directory Users and Computers.

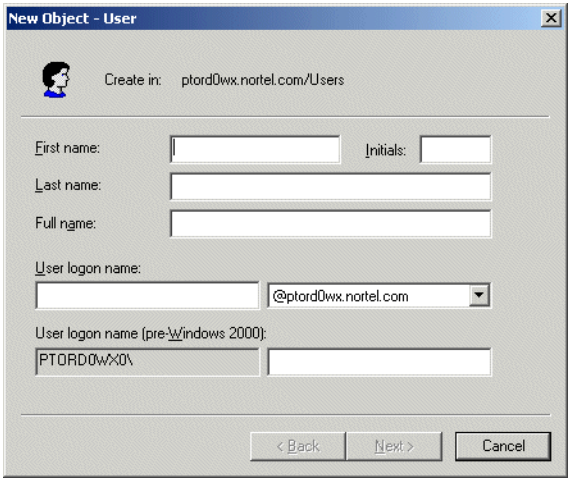
Result: The Active Directory Users and Computers window appears.



2 In the **Tree** tab, click the plus sign (+) beside the application server's domain name to expand the tree.

3 Right-click the **Users** folder, and, from the resulting pop-up menu, select New → User.

Result: The New Object - User window appears.

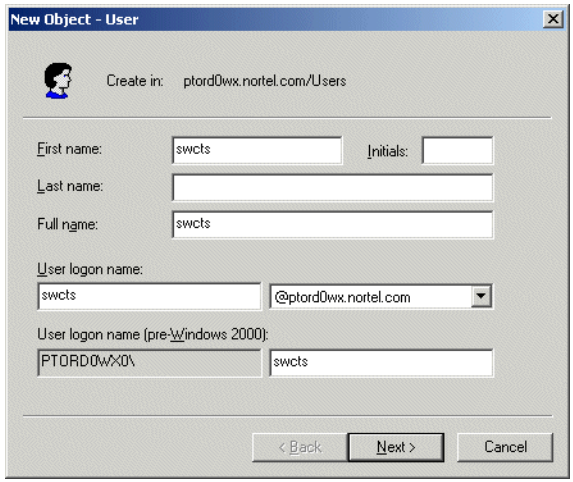


4 In the **First name** box, type the name of the user account. This is the display name that appears in the Active Directory Users and Computers window. In this example, the account is called *swcts*.

Note: Optionally, you can type the last name and initial of the person who will use this account, or you can leave the Last name and Initials boxes blank.

5 In the **User logon name** box, type the ID that users are prompted to enter when logging on to the Script Manager component of Scripting (that is, if

you configure this account so users have to type the ID, in addition to the password). In this example, the ID is also *swcts*.



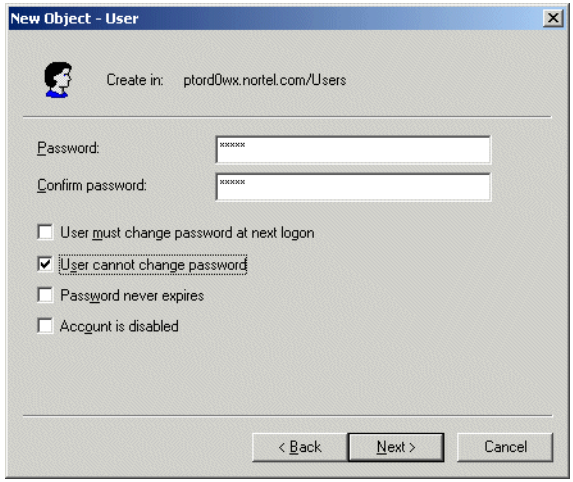
6 Click **Next**.

Result: A second New Object - User window appears.

7 In the **Password** box, type the password that users will enter when logging on to the Script Manager component of Scripting with this account.

8 In the **Confirm password** box, type the password again.

9 Click the check box beside **User cannot change password**.



10 Click **Next**.

11 The final New Object - User window appears, summarizing the account properties.

12 To create the account with these properties, click **Finish**.

Note: Click **Back** to change the account's properties.

Result: The system creates the account and it appears at the bottom of the Active Directory Users and Computers window.

13 Optionally, to add a description of the account that will appear in the Active Directory Users and Computers window, continue with this step. Otherwise, proceed to step 17. In the Active Directory Users and Computers window, right-click the new account, and then select **Properties**. In this example, you would right-click **swcts,** and then select **Properties**.

Result: The <*account name*> Properties window appears.

14 Click the **General** tab.

15 In the **Description** box, type the account description. For example, you can type "Secure Terminal Services account."

16 Click **OK** to save your changes and close the window.

17 In the Active Directory Users and Computers window, click Console → Exit to close the window.

To add the new Terminal Services account to the Domain Controller local security policy

1 Click Start → Programs → Administrative Tools → Domain Controller Security Policy.

Result: The Domain Controller Security Policy window appears.

2 In the left pane, click the plus sign (+) beside Security Settings.

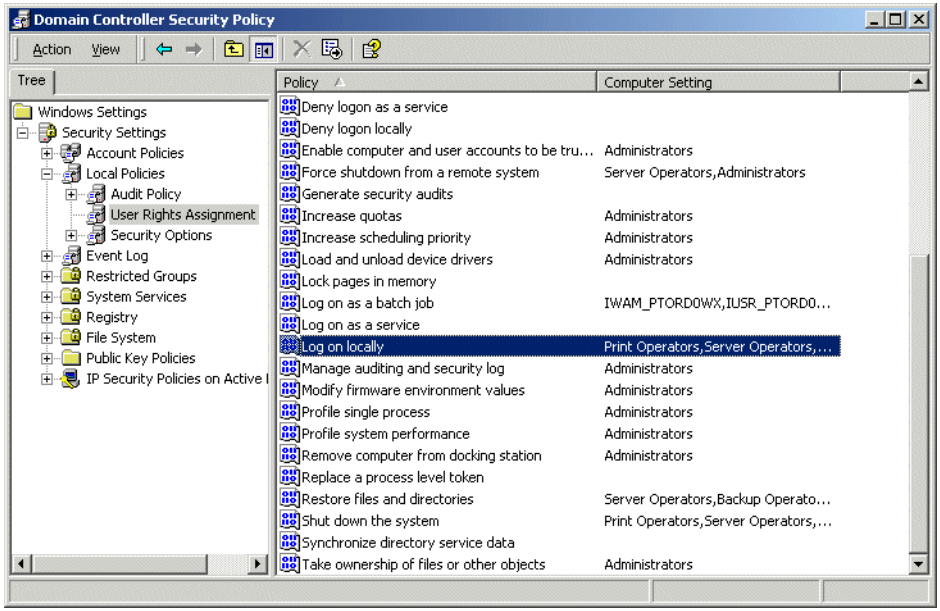
Result: The heading expands.

3 Click the plus sign (+) beside Local Policies.

Result: The heading expands.

4 Click **User Rights Assignment**.

Result: The list of local policies appears in the right pane.

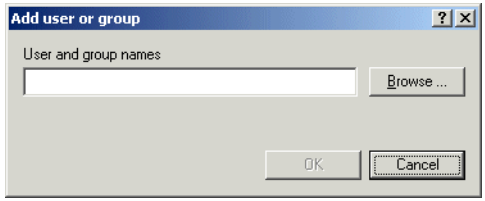


5 In the right pane, right-click the **Log on locally** policy, and then click **Security** on the resulting pop-up menu.

Result: The Security Policy Setting window appears.

6 Click **Add**.

Result: The Add user or group window appears.



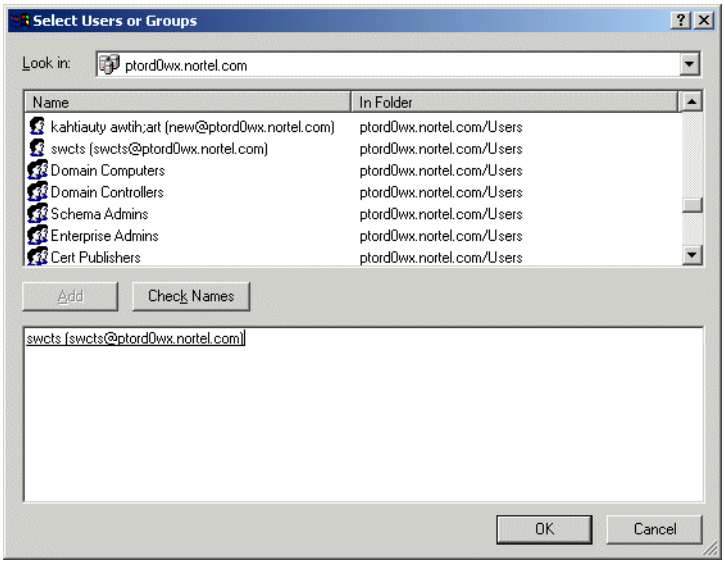
7 Click **Browse** to locate the new Active Directory user account you created.

Result: The Select Users or Groups window appears.

8 In the top portion of the window, highlight the new user you created. In this example, you would highlight the name *swcts.*

9 Click **Add**.

Result: The name appears at the bottom of the window.



10 Click **OK** to save your changes and close the Select Users or Groups window.

11 Click **OK** to close the Add user or group window.

Result: The account name appears in the Security Policy Setting window.

12 Click **OK** to save your changes and close this window.

13 Close the Domain Controller Security Policy window.

To grant the required file and directory permissions to the new user account

In this procedure, you must add the new account (in this example, *swcts*) and grant the required permissions to the following file and directory:

- the root directory where the operating system is installed, for example the C: drive
- the Symposium Web Client file *nicmisc.mdb*, which is installed in the following directory, where C: is the drive on which you installed Symposium Web Client:

C:\Program Files\Nortel Networks\WClient\Apps\Scripting\data

1 On the application server, open Windows Explorer and navigate to the drive on which the operating system is installed (for example, the C: drive).

2 Right-click the drive letter, and, from the resulting pop-up menu, select **Properties**.

Result: The Local Disk <drive letter> Properties dialog box appears.

3 Click the **Security** tab.

4 Click **Add**.

Result: The Select Users, Computers, or Groups window appears.

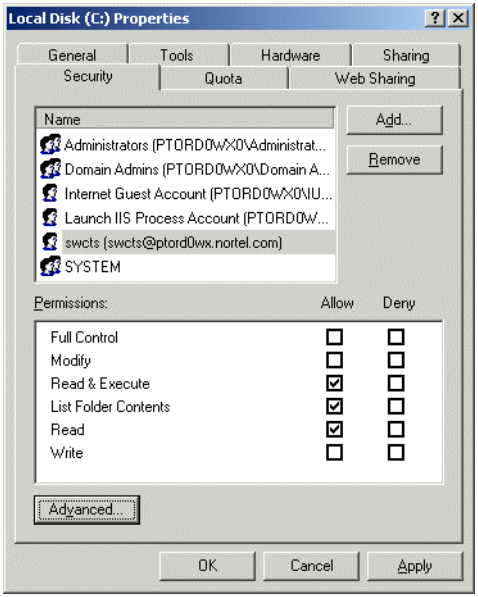
5 In the top of the window, locate the new Active Directory user account. In this example, you would locate *swcts*.

6 Double-click the account.

Result: The user account appears at the bottom of the window.

7 Click **OK**.

Result: The user account appears in the Local Disk <drive letter> Properties window.



8 In the Local Disk <drive letter> Properties window, highlight the *swcts* user account.

9 In the bottom of the window, ensure that the **Read & Execute** check box is selected in the **Allow** column.

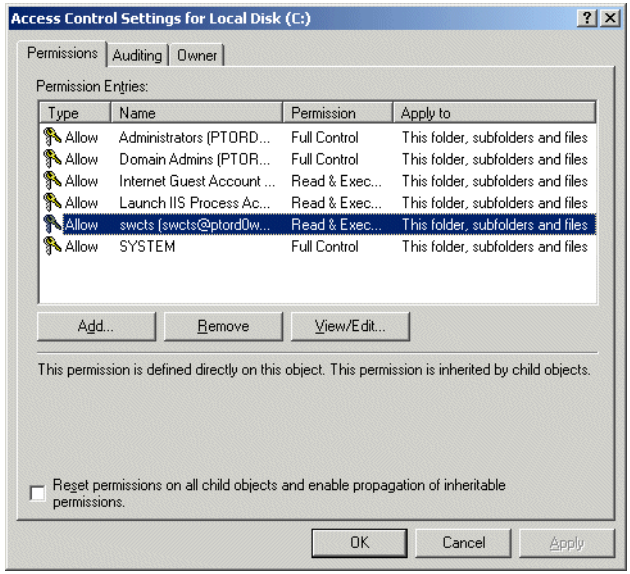
Note: When you click **Read & Execute**, it automatically includes **List Folder Contents** and **Read** permissions.

10 Ensure that all other permissions are deselected.

11 Click **Apply**.

12 Click **Advanced**.

Result: The Access Control Settings for Local Disk <drive letter> window appears.



13 Ensure that the **Apply to** text beside the new user account reads *This folder, subfolders and files*. If this value is not listed, then continue with the following step. If this value is already listed, then proceed to step 17.

14 Highlight the user account, and then click **View/Edit**.

Result: The Permission Entry for Local Disk <drive letter> window appears.

15 From the Apply onto drop-down list, select **This folder, subfolder and files**.

16 Click **OK** to save your changes and close the Permission Entry for Local Disk <drive letter> window.

17 Click **OK** to close the Access Control Settings for Local Disk <drive letter> window.

18 Click **OK** to save your changes and close the Local Disk <drive letter> Properties window.

Result: The system applies your changes. This may take a few moments. When it is finished, the <user account> Properties window appears.

19 Click **OK**.

20 In Windows Explorer, navigate to the following folder,

C:\Program Files\Nortel Networks\WClient\Apps\Scripting\data

where *C:* is the drive on which you installed Symposium Web Client.

21 In this folder, right-click the file *nicmisc.mdb*, and, from the resulting pop-up menu, select **Properties**.

Result: The nicmisc.mdb Properties dialog box appears.

22 Click the **Security** tab.

23 Click **Add**.

Result: The Select Users, Computers, or Groups window appears.

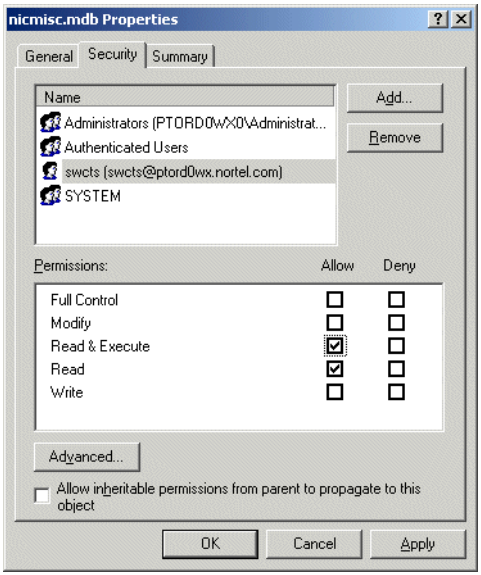
24 In the top of the window, locate the new Active Directory user account. In this example, you would locate *swcts*.

25 Double-click the account.

Result: The user account appears at the bottom of the window.

26 Click **OK**.

Result: The user account appears in the nicmisc.mdb Properties window.



27 In the nicmisc.mdb Properties window, highlight the new user account. In this example, highlight the *swcts* user account.

28 In the bottom of the window, ensure that the **Read & Execute** check box is selected in the **Allow** column.

Note: When you click **Read & Execute**, it automatically includes **Read** permissions.

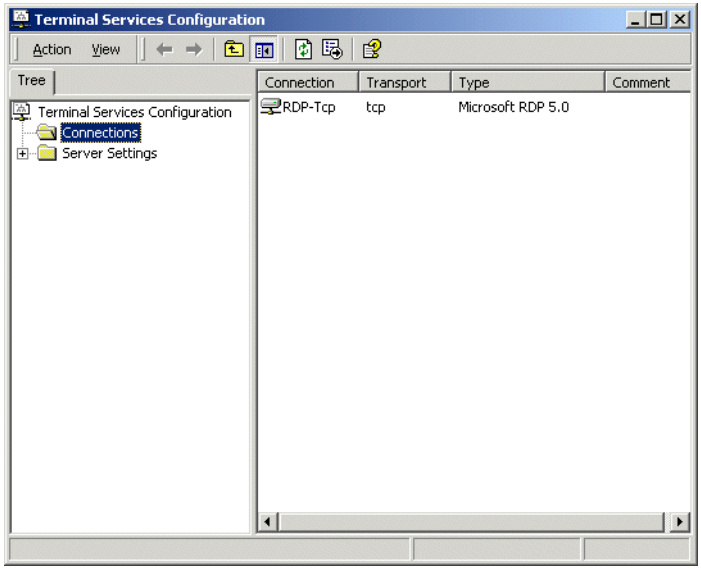
29 Ensure that all other permissions are deselected, and accept the default value for the check box beside **Allow inheritable permissions from parent to propagate to this object**.

30 Click **OK** to save your changes.

To configure Terminal Services with the new user account

1 Click Start → Programs → Administrative Tools → Terminal Services Configuration.

2 The Terminal Services Configuration window appears.



3 Double-click the **RDP-Tcp** icon in the right side of the window.

Result: The RDP-Tcp Properties window appears.

4 Click the **Logon Settings** tab.

5 You have two choices on this tab, based on the degree of security you want to configure:

- To have the system prompt users for *both* a user name and password when they launch the Script Manager portion of Scripting, click **Use client-provided logon information**. In the example followed throughout this section, if you click this option, then users have to enter *swcts* and its corresponding password to log on to the Script Manager portion of Scripting.
- To have the system prompt users for *only* the password corresponding to the new user account you created, perform the following steps:

a. Click **Always use the following logon information**.

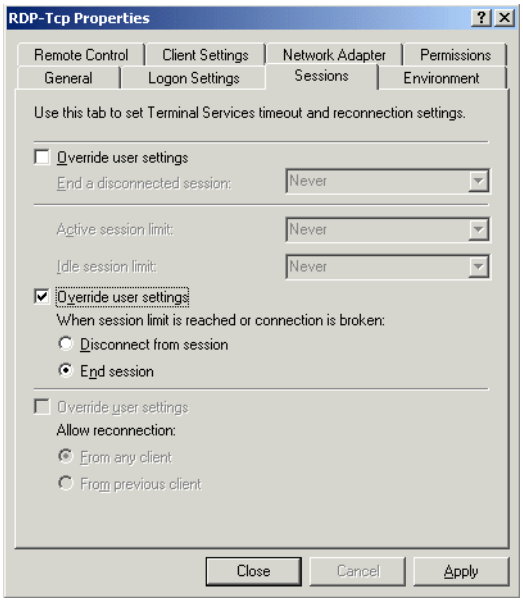
b. In the **User name** box, type the name of the new user account you created (in this example, *swcts*).

c. Leave the **Domain** box blank.

d. Ensure that the check box beside **Always prompt for password** is selected.

6 Click **Apply**.

7 Click the **Sessions** tab.



8 Click the *second* **Override user settings** check box, and then click **End session**.

9 Click **Apply**.

10 Click **Close**.

11 Exit the Terminal Services Configuration window.

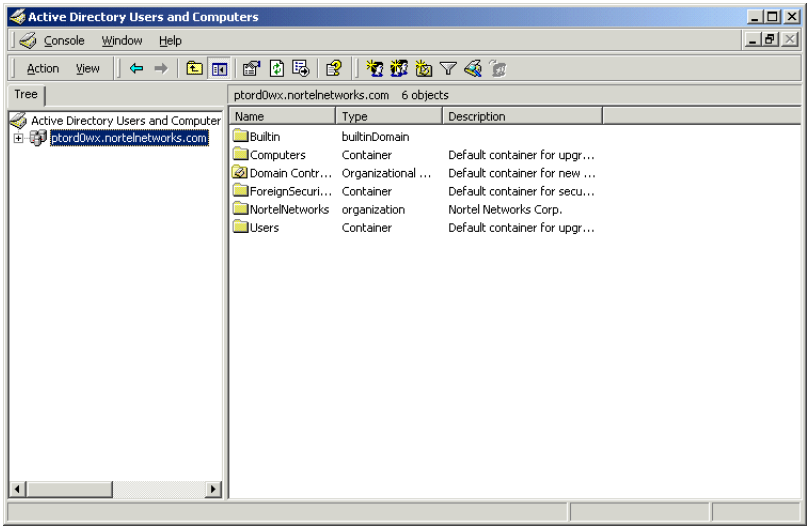
Result: Now, when users launch the Script Manager, they are prompted to type both the user ID and password of this new user account you created, or only the password, based on how you configured the account in step 5.

To disable the TsInternetUser account

Perform this procedure only if you have created an account of your choice to replace the default Active Directory user account, TsInternetUser. This procedure does not remove the TsInternetUser account from the application server. Instead, it disables it so that users can no longer log on to Terminal Services with the TsInternetUser account. However, you can still use this account to log on to the application server locally and open the files and folders to which the TsInternetUser account has access.

1 Click Start → Programs → Administrative Tools → Active Directory Users and Computers.

Result: The Active Directory Users and Computers window appears.



2 In the **Tree** tab, click the plus sign (+) beside the application server's domain name to expand the tree.

3 Click the **Users** folder.

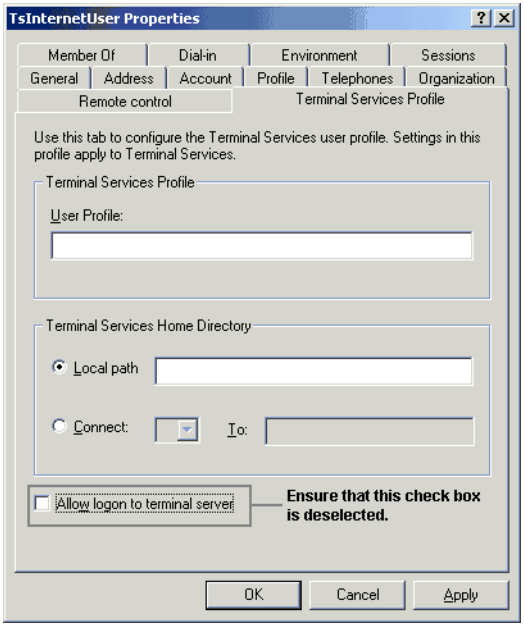
Result: The list of Active Directory users appears in the right pane.

4 In the right pane, right-click the TsInternetUser account and, from the resulting pop-up menu, click **Properties**.

Result: The TsInternetUser Properties window appears.

5 Click the **Terminal Services Profile** tab.

6 Deselect the check box beside **Allow logon to terminal server**.



7 Click **OK** to save your changes and close the properties window.

8 Close the Active Directory Users and Computers window**.**

Result: Users cannot use the TsInternetUser account to log on to Terminal Services.

What's next?

Configure your client PC. For more information, see "Installing and configuring client software" on page 287. Once you install and configure client applications, you can log on to Symposium Web Client to add and configure servers in Symposium Call Center Server using the Configuration component. See "Adding and configuring call center servers" on page 386 for more information.

Chapter 4

Installing and configuring client software

In this chapter

Installing third-party software on a client 288
Installing and configuring Agent Desktop Displays on a client PC 320

Installing third-party software on a client

Introduction

Each client PC in Symposium Web Client requires different third-party software, depending on which platform the client runs:

- Microsoft Data Access Components (MDAC) v.2.5 or later (Windows 98 clients only)
- Internet Explorer v.5.5 with Service Pack 2 (minimum), Internet Explorer v.6.0 with Service Pack 1 or later (recommended) all clients
- Windows Installer 2.0 or later. Version 2.0 is included on the Symposium Web Client CD-ROM, and in both Windows 2000 Service Pack 3 for Windows 2000 Server and Professional, and Windows XP. If the client PC runs any other operating system, then you must install the software from the Symposium Web Client CD-ROM. For more information on installing this software, see “To install Windows Installer 2.0 or later” on page 101.
- Simple Object Access Protocol (SOAP) version 3.0 merge module (a Microsoft standard component required by all clients running Windows 98, NT 4.0 Workstation, XP, Windows 2000 Professional, Windows 2000 Server, or Windows 2000 Advanced Server)
- True DB Grid Pro (all clients using Scripting). For a complete listing of the third-party controls required on the client PC, see “Third-party controls required on the client PC” on page 317.
- Terminal Services Active X Control (all clients using Scripting)

Note: You must configure the Display settings on the client PC’s monitor. Click Start → Settings → Control Panel. Double-click **Display**, and then click the **Settings** tab. In the **Font size** drop-down box, select **Small Fonts**. If you do not select **Small fonts**, some items may not display correctly in the browser.

Installing Microsoft Data Access Components

Microsoft Data Access Components (MDAC) facilitates the exchange of data between Real-Time Displays in Web Client and Symposium Call Center Server. MDAC version 2.5 or later must be installed on each client that accesses the Real-Time Reporting component. The Symposium Web Client installation CD includes MDAC version 2.5, the minimum version of the software that you require.

Note: If the client PC runs on the Windows 2000 operating system, you can skip the instructions in this section because MDAC version 2.5 is included in this operating system. Likewise, if the client runs on the Windows XP operating system, you can skip this procedure because MDAC version 2.7 is included in this operating system. However, MDAC version 2.5 is *not* included in Windows 98 or Windows NT 4 SP 6a Workstation, so you must install the software on client PCs running on either of these platforms.

If you are uncertain whether the correct version of MDAC is installed on the client PC, perform the following procedure.

To verify that Microsoft Data Access Components v.2.5 or later is installed on a client

1 Navigate to the following path:

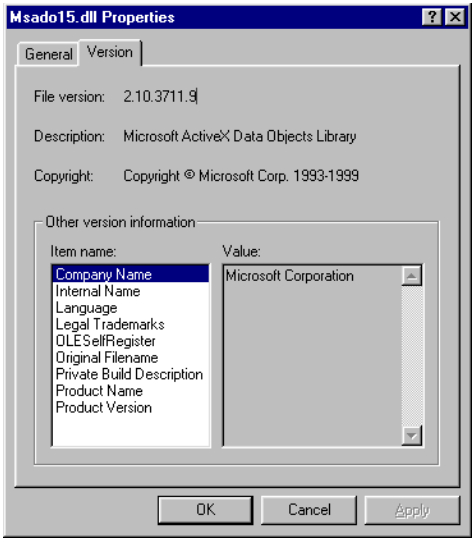
[*x:*]\Program Files\Common Files\System\ado

where *x* is the drive on which the operating system is installed.

2 Right-click the file called **msado15.dll**, and then click **Properties** on the pop-up menu.

Result: The Msado15.dll Properties window appears.

3 Click the **Version** tab, and then check the value in the **File version** field.



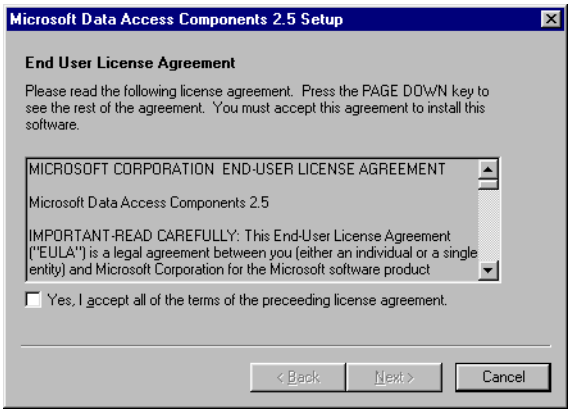
If the version number is not 2.5 or later, you must install MDAC v.2.5 on the client.

To install Microsoft Data Access Components v.2.5 on a client

1 Navigate to the Win98 ExtraInstall directory on the Symposium Web Client installation CD.

2 Double-click **Mdac25.exe**.

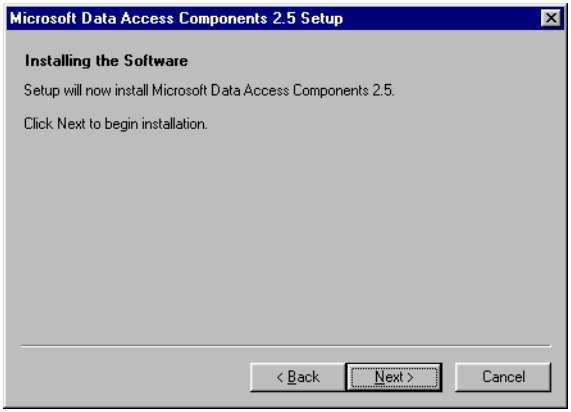
Result: The Microsoft Data Access Components 2.5 Setup window appears.



3 Click the **Yes, I accept all of the terms of the preceding license agreement** check box.

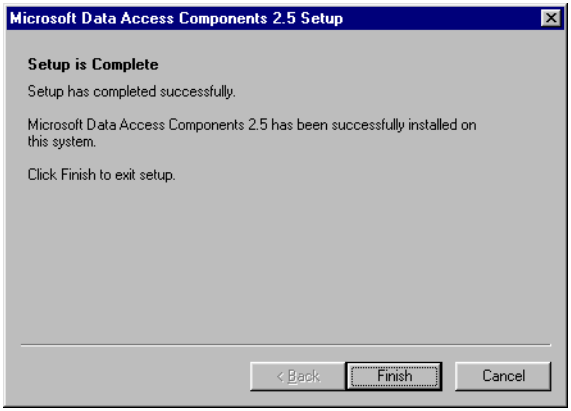
4 Click **Next**.

Result: The Installing the Software window appears.



5 Click **Next**.

Result: The Installing Components window appears. As files are copied to your system, a Copying Files dialog box appears. When all of the required files are copied, the Setup is Complete window appears.



6 Click **Finish**.

Result: MDAC v.2.5 is installed on the client.

Installing and configuring the browser on a client workstation

To access Symposium Web Client with a client PC, you must first install and configure the browser (Internet Explorer 5.5 with Service Pack 2 (minimum), Internet Explorer 6.0 with Service Pack 1 or later [recommended]) on each client workstation.

You can install Internet Explorer 5.5 Service Pack 2 (or later) directly from a CD-ROM; however, if you already have an earlier version of Internet Explorer on your PC, you need to *upgrade* to Internet Explorer 5.5 Service Pack 2 or later first, and then install the Service Pack. You can obtain the Internet Explorer 5.5 upgrade and Service Pack on CD-ROM from Microsoft. Or. if you have Internet access, you can upgrade to Internet Explorer 6.0 with Service Pack 1 or later using the Update Information link on the Help → About Internet Explorer menu (you cannot upgrade to Internet Explorer 5.5 Service Pack 2 through the Internet).

The following procedure outlines how to upgrade Internet Explorer through this Microsoft utility on the Internet. However, when you perform this procedure, the utility only enables you to upgrade to Internet Explorer version 6.0 Service Pack 1 (or later). While you can still run Symposium Web Client on Internet Explorer version 5.5 Service Pack 2, you can only upgrade to this version if you have the software saved on CD-ROM.

To upgrade Internet Explorer on the client PC

1 Open Internet Explorer, and then click Help → About Internet Explorer on the menu.

Result: The About Internet Explorer window appears.

2 Click **Update Information**.

Result: The Internet Explorer Home Page appears in the browser.

3 Click **Download**.

Result: The Microsoft Windows Update for Internet Explorer page appears.

4 Scroll down to the **Recommended Updates** section of the page, and then click the latest Internet Explorer 6.0 Service Pack.

Result: The Internet Tools page appears.

5 Select the language version of your choice, and then click **Download Now**.

Result: The File Download dialog box appears with **Save this program to disk** selected by default.

6 Click **Run this program from its current location**, and then click **OK**.

Result: The Security Warning dialog box appears, prompting you to confirm your decision to install and run the program.

7 Click **Yes**.

8 The Welcome to Setup for Internet Explorer and Internet Tools window appears.

9 Click **I accept the agreement**, and then click **Next**.

Result: The Initializing Setup window appears briefly and is replaced by the Windows Update: Internet Explorer and Internet Tools window with **Install Now - Typical set of components** selected as the default.

10 Click **Next**.

Result: The Preparing Setup window appears.

11 Click **Next**.

12 The Download Sites window appears.

13 Select the region from which Windows should get any additional files, and then click **Next**.

Result: The Progress window appears and the installation begins. When the installation is complete, the Restart Computer window appears.

14 Click **Finish** to restart your system.

Configuring Internet Explorer

Within this section are instructions for configuring Internet Explorer 5.5 (with Service Pack 2) or Internet Explorer 6.0 with Service Pack 1. Choose the section that is appropriate for your organization.

The instructions for Internet Explorer 5.5 (with Service Pack 2) are below. To configure Internet Explorer 6.0 or later, see “To configure Internet Explorer 6.0 Service Pack 1 (or later)” on page 297.

To configure Internet Explorer 5.5 Service Pack 2 (or later)

1 Start Internet Explorer 5.5.

2 From the menu bar, select Tools → Internet Options.

Result: The Internet Options window appears.

3 Click the **Security** tab.

4 Click the **Trusted Sites** icon.

5 Click **Custom Level**.

Result: The Security Settings window for trusted sites appears.

6 Under the **ActiveX controls and plug-ins** heading, ensure that **Enable** is selected for the following ActiveX controls and plug-ins:

- Run ActiveX controls and plug-ins
- Script ActiveX controls marked safe for scripting

Ensure that **Enable** or **Prompt** is selected for the following ActiveX controls and plug-ins:

- Download signed ActiveX controls

- Initialize and script ActiveX controls not marked safe for scripting

Finally, ensure that any of the three values (**Enable**, **Prompt**, or **Disable**) is selected for the item, **Download unsigned ActiveX controls**.

Note: If you select **Prompt** for the **Download signed ActiveX controls** item, the browser displays a security warning window when you first access a web page that needs to download signed ActiveX controls to your client PC. The window displays the digital certificate used to sign the control. If you select **Prompt** for the **Initialize and script ActiveX controls not marked safe for scripting** item, the browser displays a message the first time each page loads a control that is not marked safe for scripting. The message asks if you want to allow the ActiveX control to interact with other parts of the page.

7 Under the **Cookies** heading, ensure that **Enable** is selected for all of the cookies options.

Note: If you prefer not to enable cookies on your browser or to set up the Symposium Web Client application server as a Trusted Site, then you must upgrade to Internet Explorer 6.0 or later to use Symposium Web Client. In Internet Explorer 6.0, you can still view a web site that uses cookies even when you do not enable cookies. For more information, see “To configure Internet Explorer 6.0 Service Pack 1 (or later)” on page 297.

8 Click **OK** to return to the Internet Options window.

Result: A message box appears, asking if you want to change the security settings for the zone.

9 Click **Yes**.

10 Click **Sites**.

Result: The Trusted Sites window appears.

11 Deselect the **Require server verification {https:} for all sites in this zone** check box.

12 In the **Add this Web site to the zone** box, enter the server name or IP address for your application server.

13 Click **Add**.

14 Click **OK** to return to the Internet Options window.

15 Click the **Local intranet** icon.

16 Click **Custom Level**.

Result: The Security Settings window for the local intranet appears.

17 Under the **ActiveX controls and plug-ins** heading, ensure that **Enable** is selected for the following ActiveX controls and plug-ins:

- Run ActiveX controls and plug-ins
- Script ActiveX controls marked safe for scripting

Ensure that **Enable** or **Prompt** is selected for the following ActiveX controls and plug-ins:

- Download signed ActiveX controls
- Initialize and script ActiveX controls not marked safe for scripting

Finally, ensure that any of the three values (**Enable**, **Prompt**, or **Disable**) is selected for the item, **Download unsigned ActiveX controls**.

Note: If you select **Prompt** for the **Download signed ActiveX controls** item, the browser displays a security warning window when you first access a web page that needs to download signed ActiveX controls to your client PC. The window displays the digital certificate used to sign the control. If you select **Prompt** for the **Initialize and script ActiveX controls not marked safe for scripting** item, the browser displays a message the first time each page loads a control that is not marked safe for scripting. The message asks if you want to allow the ActiveX control to interact with other parts of the page.

18 Under the Cookies heading, ensure that **Enable** is selected for all of the cookies options.

19 Click **OK**.

Result: The system displays a warning that you are about to change the security settings for the zone.

20 Click **Yes**.

21 Click the **Advanced** tab.

22 Under **Browsing**, deselect the **Reuse windows for launching shortcuts** check box.

23 Click **OK** to exit the Internet Options window.

24 Restart Internet Explorer 5.5 to activate the changes.

To configure Internet Explorer 6.0 Service Pack 1 (or later)

When you configure Internet Explorer 6.0 with Service Pack 1 or later you do not have to enable all cookies to view web sites that use cookies (such as Symposium Web Client). Instead, Internet Explorer 6.0 enables you to view these web sites by either configuring them as Trusted Sites and disabling cookies, or by customizing the cookie handling for these particular sites.

When you configure Internet Explorer version 6.0 Service Pack 1 or later, you have three configuration options. The step-by-step procedures for each option follow.

- **Option 1** Configure the application server as a Trusted Site and either disable all cookies, or block cookies to the desired level of security.
- **Option 2** Do not configure the application server as a Trusted Site, but override cookie handling for the application server. With this option, you can use advanced cookie handling to disable session cookies.
- **Option 3** Do not configure the application server as a Trusted Site and do not override cookie handling for the application server. Instead, set the slider on the Privacy tab to High, or use the advanced cookies settings to set the desired security level. In this latter case, however, you must select **Always allow session cookies**.

Option 1 - To configure Internet Explorer 6.0 (with the application server set as a Trusted Site)

Perform the following procedure to configure Internet Explorer 6.0 and later on the client PC. In this procedure, you set the application server as a Trusted Site and you disable all cookies, or set the cookie handling to the desired level of security.

1. Start Internet Explorer 6.0 or later.
2. From the menu bar, select Tools → Internet Options.

   Result: The Internet Options window appears.
3. Click the **Security** tab.
4. Click the **Trusted Sites** icon.
5. Click **Custom Level**.

   Result: The Security Settings window for trusted sites appears.

6 Under the **ActiveX controls and plug-ins** heading, ensure that **Enable** is selected for the following ActiveX controls and plug-ins:

- Run ActiveX controls and plug-ins
- Script ActiveX controls marked safe for scripting

Ensure that **Enable** or **Prompt** is selected for the following ActiveX controls and plug-ins:

- Download signed ActiveX controls
- Initialize and script ActiveX controls not marked safe for scripting

Finally, ensure that any of the three values (**Enable**, **Prompt**, or **Disable**) is selected for the item, **Download unsigned ActiveX controls**.

Note: If you select **Prompt** for the **Download signed ActiveX controls** item, the browser displays a security warning window when you first access a web page that needs to download signed ActiveX controls to your client PC. The window displays the digital certificate used to sign the control. If you select **Prompt** for the **Initialize and script ActiveX controls not marked safe for scripting** item, the browser displays a message the first time each page loads a control that is not marked safe for scripting. The message asks if you want to allow the ActiveX control to interact with other parts of the page.

7 Click **OK**.

Note: If you have enabled any ActiveX options, a message box appears, asking you to confirm your choice. Click **Yes**.

8 Click the **Privacy** tab to choose the way you want to handle cookies:

- To disable all cookies, drag the slider to the top of the ruler until Block All Cookies appears at the top.
- Alternatively, drag the slider to any of the levels in the middle of the ruler until you reach the desired privacy setting.

9 Click **Apply.**

10 Click the **Security** tab.

11 Click the **Trusted Sites** icon.

12 Click **Sites**.

Result: The Trusted sites window appears.

13 Deselect the **Require server verification {https:} for all sites in this zone** check box.

14 In the **Add this Web site to the zone** box, enter the server name or IP address for your application server.

15 Click **Add**.

16 Click **OK** to return to the Internet Options window.

17 Click the **Local intranet** icon.

18 Click **Custom Level**.

Result: The Security Settings window for the local intranet appears.

19 Under the **ActiveX controls and plug-ins** heading, ensure that **Enable** is selected for the following ActiveX controls and plug-ins:

- Run ActiveX controls and plug-ins
- Script ActiveX controls marked safe for scripting

Ensure that **Enable** or **Prompt** is selected for the following ActiveX controls and plug-ins:

- Download signed ActiveX controls
- Initialize and script ActiveX controls not marked safe for scripting

Finally, ensure that any of the three values (**Enable**, **Prompt**, or **Disable**) is selected for the item, **Download unsigned ActiveX controls**.

Note: If you select **Prompt** for the **Download signed ActiveX controls** item, the browser displays a security warning window when you first access a web page that needs to download signed ActiveX controls to your client PC. The window displays the digital certificate used to sign the control. If you select **Prompt** for the **Initialize and script ActiveX controls not marked safe for scripting** item, the browser displays a message the first time each page loads a control that is not marked safe for scripting. The message asks if you want to allow the ActiveX control to interact with other parts of the page.

20 Click **OK**.

Note: If you have enabled any ActiveX options, a message box appears, asking you to confirm your choice. Click **Yes**.

21 Click the **Advanced** tab.

22 Under **Browsing**, deselect the **Reuse windows for launching shortcuts** check box.

23 Click **OK** to exit the Internet Options window.

24 Restart Internet Explorer 6.0 to activate your changes.

Option 2 - To configure Internet Explorer 6.0 (do not set the application server as a Trusted Site and override cookie handling)

Perform the following procedure to configure Internet Explorer 6.0 and later on the client PC. In this procedure, you do not configure the application server as a Trusted Site, and you override cookie handling for the application server. With this option, you can use advanced cookie handling to disable session cookies.

1 Start Internet Explorer 6.0 or later.

2 From the menu bar, select Tools → Internet Options.

Result: The Internet Options window appears.

3 Click the **Security** tab.

4 Click the **Internet** icon.

5 Click **Custom Level**.

Result: The Security Settings window for the Internet appears.

6 Under the **ActiveX controls and plug-ins** heading, ensure that **Enable** is selected for the following ActiveX controls and plug-ins:

- Run ActiveX controls and plug-ins
- Script ActiveX controls marked safe for scripting

Ensure that **Enable** or **Prompt** is selected for the following ActiveX controls and plug-ins:

- Download signed ActiveX controls
- Initialize and script ActiveX controls not marked safe for scripting

Finally, ensure that any of the three values (**Enable**, **Prompt**, or **Disable**) is selected for the item, **Download unsigned ActiveX controls**.

Note: If you select **Prompt** for the **Download signed ActiveX controls** item, the browser displays a security warning window when you first access a web page that needs to download signed ActiveX controls to your client PC. The window displays the digital certificate used to sign the control. If you select **Prompt** for the **Initialize and script ActiveX controls not marked safe for scripting** item, the browser displays a message the first time each page loads a control that is not marked safe for scripting. The message asks if you want to allow the ActiveX control to interact with other parts of the page.

7 Click **OK**.

Note: If you have enabled any ActiveX options, a message box appears, asking you to confirm your choice. Click **Yes**.

8 Click the **Local intranet** icon.

9 Click **Custom Level**.

Result: The Security Settings window for the local intranet appears.

10 Under the **ActiveX controls and plug-ins** heading, ensure that **Enable** is selected for the following ActiveX controls and plug-ins:

- Run ActiveX controls and plug-ins
- Script ActiveX controls marked safe for scripting

Ensure that **Enable** or **Prompt** is selected for the following ActiveX controls and plug-ins:

- Download signed ActiveX controls
- Initialize and script ActiveX controls not marked safe for scripting

Finally, ensure that any of the three values (**Enable**, **Prompt**, or **Disable**) is selected for the item, **Download unsigned ActiveX controls**.

Note: If you select **Prompt** for the **Download signed ActiveX controls** item, the browser displays a security warning window when you first access a web page that needs to download signed ActiveX controls to your client PC. The window displays the digital certificate used to sign the control. If you select **Prompt** for the **Initialize and script ActiveX controls not marked safe for scripting** item, the browser displays a message the first time each page loads a control that is not marked safe for scripting. The message asks if you want to allow the ActiveX control to interact with other parts of the page.

11 Click **OK**.

Note: If you have enabled any ActiveX options, a message box appears, asking you to confirm your choice. Click **Yes**.

12 Click the **Privacy** tab to override cookie handling for the application server web site.

13 Click **Edit**.

Note: The **Edit** button is disabled if the slider is set to either **Block All Cookies** or **Accept All Cookies**. To enable the **Edit** button, move the slider to the desired level between these two settings.

Result: The Per Site Privacy Actions window appears.

14 In the **Address of Web Site** box, type the IP address of the Symposium Web Client application server.

15 Click **Allow** to enable your browser to always accept cookies for the application server.

16 Click **OK.**

17 Click **Advanced**.

Result: The Advanced Privacy Settings window appears.

18 Select **Override automatic cookie handling**.

19 Choose the desired level of privacy for first-party and third-party cookies. To block all cookies, click **Block**.

20 To disallow session cookies, ensure the check box beside **Always allow session cookies** is unchecked.

21 Click **Apply**.

22 Click the **Advanced** tab.

23 Under **Browsing**, deselect the **Reuse windows for launching shortcuts** check box.

24 Click **OK** to exit the Internet Options window.

25 Restart Internet Explorer 6.0 to activate your changes.

Option 3 - To configure Internet Explorer 6.0 (do not set the application server as a Trusted Site, do not override cookie handling for the application server, but set the privacy to High and always allow session cookies)

Perform the following procedure to configure Internet Explorer 6.0 with Service Pack 1 and later on the client PC. In this procedure, you do not configure the application server as a Trusted Site, nor do you override cookie handling for the application server. However, you set the privacy level for cookies to High, or you use the advanced cookie options to override cookie handling (in which case you must always allow session cookies).

1. Start Internet Explorer 6.0 or later.
2. From the menu bar, select Tools → Internet Options.

   Result: The Internet Options window appears.
3. Click the **Security** tab.
4. Click the **Internet** icon.
5. Click **Custom Level**.

   Result: The Security Settings window for the internet appears.
6. Under the **ActiveX controls and plug-ins** heading, ensure that **Enable** is selected for the following ActiveX controls and plug-ins:

   - Run ActiveX controls and plug-ins
   - Script ActiveX controls marked safe for scripting

   Ensure that **Enable** or **Prompt** is selected for the following ActiveX controls and plug-ins:

   - Download signed ActiveX controls
   - Initialize and script ActiveX controls not marked safe for scripting

   Finally, ensure that any of the three values (**Enable**, **Prompt**, or **Disable**) is selected for the item, **Download unsigned ActiveX controls**.

   Note: If you select **Prompt** for the **Download signed ActiveX controls** item, the browser displays a security warning window when you first access a web page that needs to download signed ActiveX controls to your client PC. The window displays the digital certificate used to sign the control. If you select **Prompt** for the **Initialize and script ActiveX controls not marked safe for scripting** item, the browser displays a message the first time each page loads a control that is not marked safe for scripting. The message asks if you want to allow the ActiveX control to interact with other parts of the page.
7. Click **OK**.

   Note: If you have enabled any ActiveX options, a message box appears, asking you to confirm your choice. Click **Yes**.
8. Click the **Local intranet** icon.
9. Click **Custom Level**.

   Result: The Security Settings window for the local intranet appears.

10 Under the **ActiveX controls and plug-ins** heading, ensure that **Enable** is selected for the following ActiveX controls and plug-ins:

- Run ActiveX controls and plug-ins
- Script ActiveX controls marked safe for scripting

Ensure that **Enable** or **Prompt** is selected for the following ActiveX controls and plug-ins:

- Download signed ActiveX controls
- Initialize and script ActiveX controls not marked safe for scripting

Finally, ensure that any of the three values (**Enable**, **Prompt**, or **Disable**) is selected for the item, **Download unsigned ActiveX controls**.

Note: If you select **Prompt** for the **Download signed ActiveX controls** item, the browser displays a security warning window when you first access a web page that needs to download signed ActiveX controls to your client PC. The window displays the digital certificate used to sign the control. If you select **Prompt** for the **Initialize and script ActiveX controls not marked safe for scripting** item, the browser displays a message the first time each page loads a control that is not marked safe for scripting. The message asks if you want to allow the ActiveX control to interact with other parts of the page.

11 Click **OK**.

Note: If you have enabled any ActiveX options, a message box appears, asking you to confirm your choice. Click **Yes**.

12 Click the **Privacy** tab.

13 Choose the level of cookie handling:

a. Drag the slider to **High.**

OR

a. To override automatic cookie handling, click **Advanced**.

Result: The Advanced Privacy Settings window appears.

b. Select **Override automatic cookie handling**.

c. Click the desired level of security for first-party and third-party cookies.

d. Select **Always allow session cookies**.

e. Click **OK**.

14 Click **Apply.**

15 Click the **Advanced** tab.

16 Under **Browsing**, deselect the **Reuse windows for launching shortcuts** check box.

17 Click **OK** to exit the Internet Options window.

18 Restart Internet Explorer 6.0 to activate your changes.

Installing Simple Object Access Protocol

Previous versions of Symposium Web Client used Remote Data Service (RDS) technology for retrieving data through client PCs from the application server. However, in Symposium Web Client 4.5 and later, this method of data retrieval is no longer applicable.

For Symposium Web Client 4.5 (and later) to function correctly, you must install a software package containing Simple Object Access Protocol (SOAP) components. You must perform this installation on every client PC that accesses the application server and that runs any one of the following operating systems:

- Windows 98, Windows NT 4.0 Workstation, Windows XP, Windows 2000 Professional, Windows 2000 Server, or Windows 2000 Advanced Server

SOAP provides a means of communication between applications running on different operating systems, with different technologies and programming languages.

To install Simple Object Access Protocol

When you use the client PC to connect to an application server running Symposium Web Client 4.5, the system checks whether the client PC contains the required SOAP files. If SOAP 3.0 is not installed, then a warning message appears, followed by a series of windows that enable you to download and install the SOAP files directly from the application server. You have three choices: you can click **Cancel** to download it later; you can save the software to the client PC's hard disk for later installation; or you can install the software immediately.

Only users who are logged on to the client PC with administrator privileges can install the software. If a user without administrator privileges is logged on to the client PC, then he or she has the option of downloading and saving the **ClientSOAP.msi** file to the client PC's hard drive. An administrator can then install the software later by double-clicking this file. However, note that you cannot use Symposium Web Client until the client SOAP software is installed.

Note: You only need to perform this installation once on each client PC, regardless of the number of Symposium Web Client upgrades you install afterward.

1 On the client PC, open Internet Explorer.

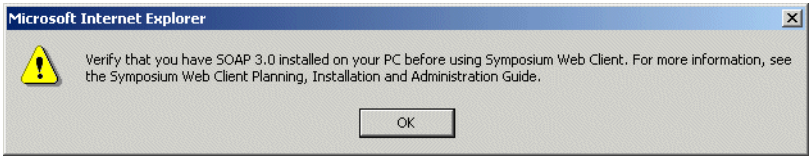
2 In the **Address** box, type the URL address of the application server. The default URL address is http://<*Application Server*>.

3 Press **Enter**.

Result: The application server displays the Symposium Web Client main logon window.

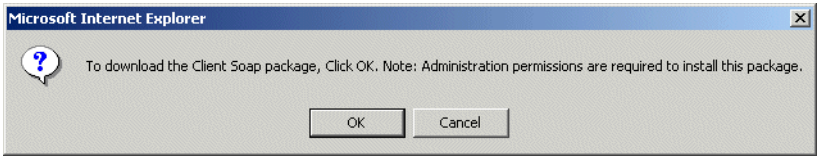
4 In the **User Name** and **Password** boxes, type your logon details, and then click **Login**.

Result: A warning message appears, notifying you that you must have SOAP 3.0 installed on the client PC.



5 Click **OK**.

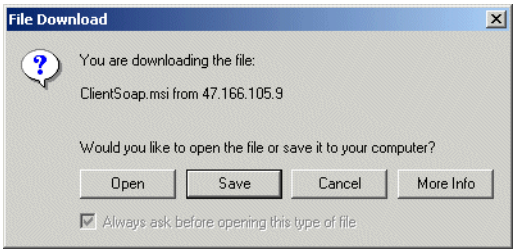
Result: A message box appears, enabling you to download the SOAP package.



6 Click **OK** to download the SOAP software.

Note: Click **Cancel** if you want to download the software at a later date. Symposium Web Client will not function properly until you install SOAP on the client PC.

Result: A window appears, enabling you to download and install the SOAP files immediately, or save the files to the client PC for a later installation.



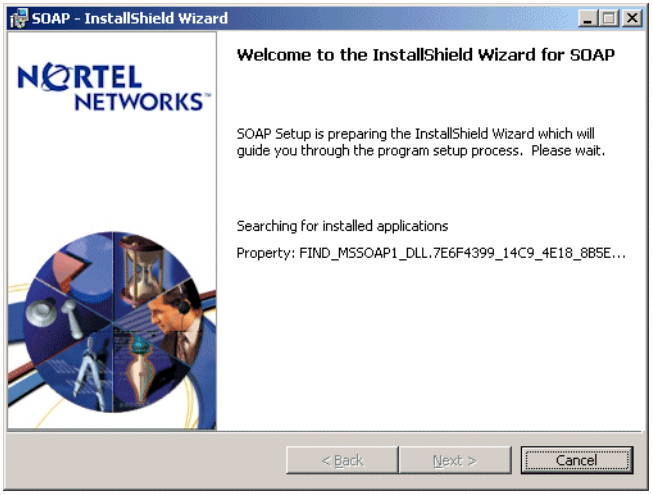
7 Click **Open** to begin the installation. You must be logged on with administrator privileges to install the SOAP software.

Note: If you prefer to save the SOAP installation file, **ClientSOAP.msi**, to the client PC for a later installation, click **Save**. A window appears, enabling you to choose the location where you want to save the file. A user with administrator privileges must double-click this file to install the software on the client PC. For installation instructions, proceed with the next Result.

Result: The installation program verifies the operating system and setup of the client PC and notifies you if you need to update the Windows Installer software.

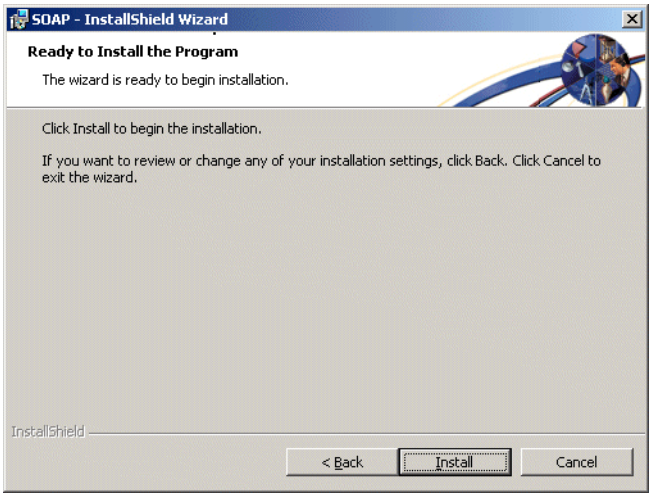
- If you need to update the Windows Installer package, you can install the software from the Symposium Web Client CD-ROM. For more information, see “To install Windows Installer 2.0 or later” on page 101. After you update the Windows Installer, you must restart the PC.
- If you do not have to update the installer, proceed to the following step.

8 The SOAP installation proceeds and the welcome window appears. You may have to wait a few moments while the program searches for installed applications, as shown in the following graphic:



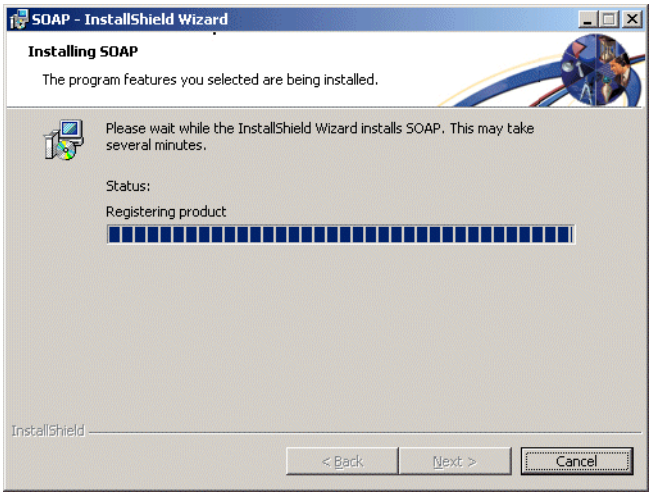
9 When the program finds the required applications, click **Next**.

Result: The Ready to Install the Program window appears.



10 Click **Install**.

Result: The Installing SOAP window appears.



11 The program installs the required SOAP components. When it is finished, the InstallShield Wizard Completed window appears.

12 Click **Finish**

Installing third-party controls on a client

Most of the Symposium Web Client components require the installation of third-party controls on the client PC. These controls are automatically downloaded and installed on the client PC the first time they are required by the Symposium Web Client application in which you are working, unless the control is already installed on the client PC. The system automatically upgrades these controls if a newer version of the control is detected on the application server, only up to the version specified by Symposium Web Client.

Third-party controls are required for all components except Configuration and Audit Trail. For information on viewing the controls that are installed on the client PC, see “To view the list of installed third-party controls” on page 319.

All the downloaded controls used by Symposium Web Client are contained in .cab files that are digitally signed. Therefore, if you configured Internet Explorer according to the procedure in the previous section, and enabled the downloading of signed ActiveX controls, the browser does not notify you that it is downloading a required control; the third-party control is automatically downloaded to the client PC.

Third-party controls and your local security policy

If the client PC runs Windows 2000, then based on the local settings of the security policy *Unsigned non-driver installation behavior* on the PC, warning windows other than those resulting from the settings you chose when configuring Internet Explorer may appear, or the required third-party controls may not be downloaded at all.

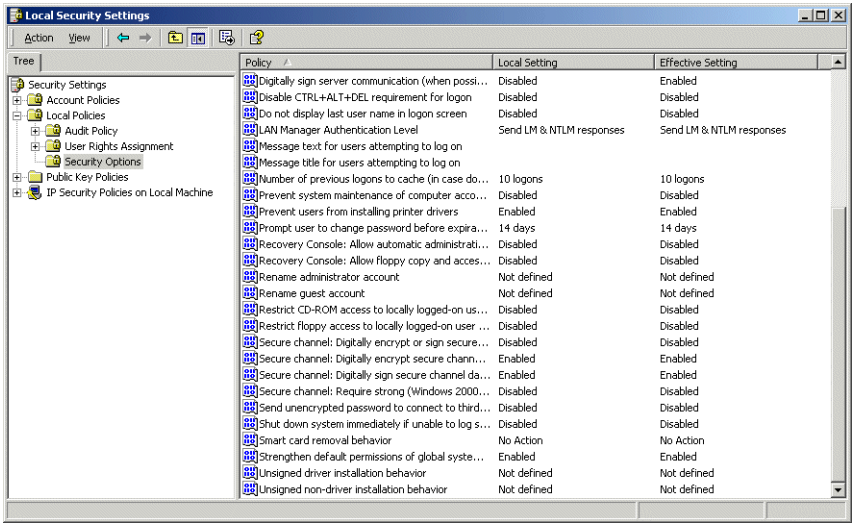
It is important, therefore, that you verify your local security settings for this policy, according to the following procedure. This procedure is only applicable to client PCs running Windows 2000. If your client PC runs any other operating system, then the security policy does not affect the downloading of third-party controls.

To verify your local security policy settings

Note: The following procedure is applicable only to Windows 2000. If your client PC runs any other operating system, then the security policy does not affect the downloading of third-party controls and you do not need to perform this procedure.

1 Click Start → Programs → Administrative Tools → Local Security Policy.

Result: The Local Security Settings window appears.



2 Click the plus sign (+) beside Local Policies.

Result: The heading expands to reveal a series of folders.

3 Click the **Security Options** folder.

Result: A series of policies appears in the right pane.

4 In the right pane, scroll down to the *Unsigned non-driver installation behavior* policy.

5 Under the **Local Setting** column, verify the current setting for this policy. The possible values are:

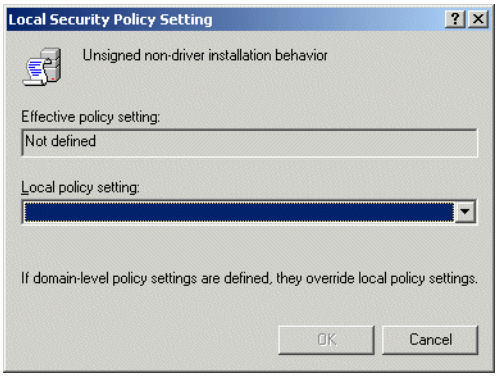
- **Not Defined** You have not configured the settings for this policy. Any warning windows that appear when you install third-party controls on the client are the result of the settings you chose when configuring Internet Explorer.
- **Silently succeed** All controls are installed on the client PC without any further warning windows, other than those resulting from the settings you chose when configuring Internet Explorer.
- **Warn but allow installation** All controls are installed on the client PC, but if any of the files within the CAB file being downloaded are not signed, then one or more warning windows appear, in addition to those

resulting from the settings you chose when configuring Internet Explorer.

- **Do not allow installation** You cannot download and install unsigned controls on the client PC, regardless of the settings you chose when configuring Internet Explorer.

6 To change the setting that appears, right-click this policy, and select **Security** from the resulting pop-up menu.

Result: The Local Security Policy Settings window appears.



7 From the **Local policy setting** drop-down list, select the new policy setting.

8 Click **OK** to save your changes.

9 Close the Local Security Settings window.

To install third-party controls on a client PC

The installation procedure in this section uses the example of how to install the third-party client controls required for Scripting (True DBGrid Pro and the Remote Desktop ActiveX control). However, the same basic procedure applies for installing any of the third-party controls for the other components:

1. You must first log on to the application server and start the applicable component.

2. Then, open the window or feature of the component that requires the third-party control. For example, True DBGrid Pro is only required for the application thresholds portion of Scripting and is, therefore, only downloaded when you open this feature in Scripting.

3. When the security warning window appears notifying you that you must install the control, click **Yes**. The system automatically installs the control (if you have set Internet Explorer to **Prompt** for Download signed ActiveX controls).

Notes:

- When downloading the control for Historical Reporting, the Crystal Reports Viewer, you may be prompted to install certain dependency files (if these files do not already exist on the PC). For details, see "To download the files required by the Crystal Reports Viewer" on page 316.
- For a complete list of the third-party controls required on the client PC, see "Third-party controls required on the client PC" on page 317.
- Both regular Windows users and domain users who log on to client PCs running either Windows XP or Windows 2000 Professional require at minimum Power User privileges on the client PC to successfully download and install many of the third-party controls required by Symposium Web Client. (A user with administrator privileges must first install client SOAP on the client PCs.) For information on giving these users the Power User privilege, consult the Microsoft Windows Help in either Windows XP or Windows 2000 Professional.

ATTENTION

You require separate licenses for Terminal Services for each client PC using the Script Editor portion of the Scripting component.

To install True DBGrid Pro on a client

When you run Scripting in Internet Explorer for the first time, the system prompts you to install True DBGrid Pro if it is not already installed on the client PC.

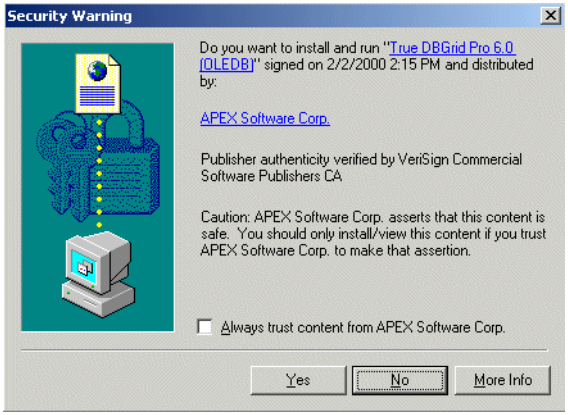
1 Log on to Symposium Web Client.

Note: For more information about logging on to Symposium Web Client for the first time, see "To log on to Symposium Web Client for the first time" on page 378.

Result: The Launch Pad appears.

2 Click **Scripting**.

Result: When the Scripting window opens in your browser, the system prompts you to install the True DBGrid Pro Control.



3 Click **Yes**.

Result: The system installs True DBGrid Pro.

To install Remote Desktop Active X Control on a client

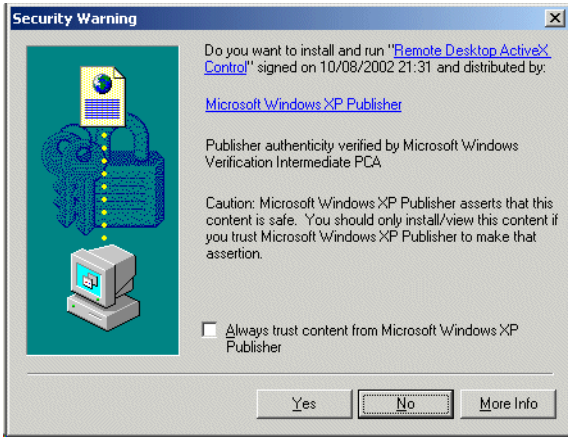
When you run Scripting in Internet Explorer for the first time, the system prompts you to install Remote Desktop Active X Control if it is not already installed.

1 Log on to Symposium Web Client.

Note: For more information about logging on to Symposium Web Client for the first time, see “To log on to Symposium Web Client for the first time” on page 378.

Result: The Launch Pad appears.

2 Click **Scripting**. When the Scripting window opens in your browser, the Security Warning dialog box for Remote Desktop ActiveX Control appears.



3 Click **Yes**.

Result: The system installs the Remote Desktop ActiveX Control.

Note: This installation of Terminal Services provides you with the Terminal Services software for a 90-day evaluation period only. Before the 90 days expire, you must purchase a Terminal Services Client Access License from Microsoft to continue to use the Scripting component beyond the evaluation period. The Scripting component does not work without Terminal Services.

Downloading the Crystal Reports Viewer

Before you can successfully run and view historical reports, the client PC must have the Crystal Reports Viewer third-party control installed. For this control to function correctly, it requires that the certain files be installed on the PC. While most of these files are downloaded automatically, the system notifies you that it needs to download the following files:

- atl.dll
- MFC.DLLs

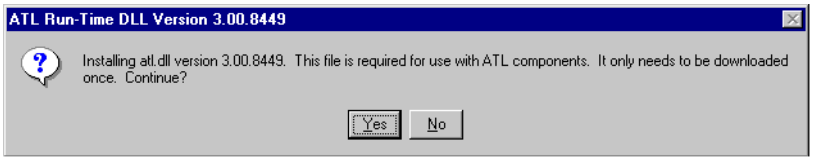
If these files are not installed when you first download the Crystal Reports Viewer, then messages appear, notifying you that you must install them, as outlined in the following procedure.

To download the files required by the Crystal Reports Viewer

1 On the client PC, open the Historical Reporting component.

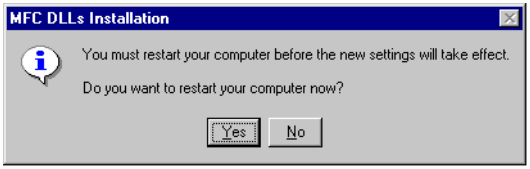
2 Run an ad hoc report.

Result: The system downloads the Crystal Reports Viewer. Then, if the required *atl* file for this Viewer is not installed, the report viewer appears blank and the following message box appears:



3 Click **Yes** to install the file.

Result: The system installs the file and a message appears, prompting you to restart the PC.

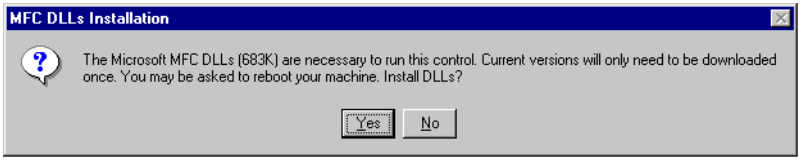


4 Click **Yes** to restart the PC, or **No** to restart later.

Note: You do not have to restart the PC for these changes to take effect.

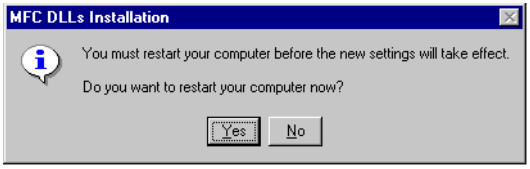
5 On the client PC, try to run the ad hoc report again.

Result: If the report is generated successfully, then you do not have to continue with the following steps and you are finished this procedure. However, if the required *mfc* files are not installed, then the report viewer appears blank and the following message box appears:



6 Click **Yes** to install the files.

Result: The system installs the required files and a message box appears, prompting you to restart your PC.



7 Click **Yes** to restart the PC, or **No** to restart later.

Note: You do not have to restart the PC for these changes to take effect.

Result: On the client PC, you can now run the ad hoc report successfully.

Third-party controls required on the client PC

Notes:

- **Deleting controls** You can safely delete any of the controls from the client PC. However, note that if Internet Explorer has been using the control, you may need to close the browser and reopen it before the system allows you to delete the control.
- **Installing later versions** If you delete a control, and then subsequently require it again to work in Symposium Web Client, sometimes Internet Explorer only offers you a later version of the control than that which you originally installed. You can install later versions of the controls without adversely affecting Symposium Web Client. For information on viewing the version number of the controls installed on the client PC, see “To view the list of installed third-party controls” on page 319.

The following table lists all the third-party controls that must be installed on the client PC if it is used to access all Symposium Web Client 4.5 components (except Configuration and Audit Trail, which have no dependency on third-party controls). Some controls are required for more than one component, but you only need to install them once. For a complete list of the control files and their version numbers, see Appendix D, “Third-party controls required on the client PC.”

Control	Company	Purpose
Crystal Reports Viewer	Crystal Decisions	Crystal Reports
Emergency Help	Nortel Networks	Emergency Help
Popup Menu	Microsoft	Internet Explorer Popup Menu
Date and Time Picker	Microsoft	Time and date picker control
Remote Desktop Client	Microsoft	Terminal Services
Olectra Chart	ComponentOne	Chart control
Real-time Display	Nortel Networks	Real-time displays
Sheridan ActiveTreeView	Infragistics	TreeView control
True OLE DB Grid 6	Apex Software	Grid control
Windows Scripting Shell None*	Microsoft	Reads from the registry
SOAP Client 3.0 *	Microsoft	Access to server-side functionality

*Unlike the other controls listed in the table, these two controls are not downloaded to the client PC, but they are required for proper Symposium Web Client functionality. For more information on installing the client version of SOAP, see “Installing Simple Object Access Protocol” on page 305. The control for Windows scripting is automatically installed with the client operating system.

Viewing the list of installed third-party controls

When you want to verify which third-party controls are installed on the client PC and their version numbers, you can use the Tools menu in Internet Explorer.

To view the list of installed third-party controls

1. In Internet Explorer, click Tools → Internet Options.

   Result: The Internet Options window appears.

2. On the General tab, under the Temporary Internet files heading, click **Settings**.

   Result: The Settings window appears.

3. Click **View Objects**.

   Result: The Downloaded Program Files window appears, listing the installed controls, the date they were installed, and their version numbers.

Installing and configuring Agent Desktop Displays on a client PC

Introduction

Agent Desktop Displays is a Windows-based tool that provides skillset monitoring to Symposium Call Center Server agents. Agents or supervisors can log on to Agent Displays using their phoneset logon ID and view statistics for each skillset to which they belong.

Agent Desktop Displays' tabular format appears as a window with several columns. This window can be moved, minimized, resized, closed, or set to always stay on top of the desktop like any standard Microsoft window.

Notes:

- If the client operating system is Windows NT 4.0 Workstation, Windows XP, or Windows 2000, then you must be logged on to the PC as a user with Administrator privileges to install or upgrade Agent Desktop Displays. This also applies if you are installing the client portion of Agent Desktop Displays on the application server. The Windows 98 operating system does not require Administrator privileges.
- Before you can install Agent Desktop Displays on the client PC, you must ensure that it has the Windows Installer 2.0 or later installed (version 2.0 is included on the Symposium Web Client CD-ROM, and in both Windows 2000 Service Pack 3 for Windows 2000 Server and Professional, and Windows XP). For more information on installing this software from the Symposium Web Client CD-ROM, see "To install Windows Installer 2.0 or later" on page 101.
- For information on upgrading Agent Desktop Displays from Release 4.0 to 4.5, see "Upgrading the Agent Desktop Displays client software" on page 352.

Versions of Agent Desktop Displays and compatibility with Symposium Web Client

If you are going to use Agent Desktop Displays on a client PC that connects to multiple application servers, then you must ensure that each application server has the same version of Symposium Web Client installed.

- **Agent Desktop Displays 4.5 connecting to Symposium Web Client 4.0**
  The Agent Desktop Displays 4.5 client software is incompatible with the Symposium Web Client 4.0 software that is installed on the application server. Once you upgrade the client PC from Agent Desktop Displays Release 4.0 to Release 4.5, then you cannot use the Agent Desktop Displays component when the client PC connects to an application server running Symposium Web Client 4.0.
- **Agent Desktop Displays 4.0 connecting to Symposium Web Client 4.5**
  Agent Desktop Displays Release 4.0 is compatible with an application server running Release 4.5. When you use a client PC running Agent Desktop Displays Release 4.0 to connect to an application server running Symposium Web Client Release 4.5, a message appears, notifying you that there is a newer version of the client software available and enabling you to upgrade the software to Release 4.5.

  If you choose not to upgrade, then you can continue to use Agent Desktop Displays Release 4.0. However, in this case, the communication between the client PC and application server continues to be through Remote Data Service (RDS), rather than SOAP, which is new to Release 4.5. Therefore, the RDS communication method must be enabled on the application server for Agent Desktop Displays 4.0 to function properly. For details on enabling RDS, see “To reenable Remote Data Service” on page 244. For information on upgrading Agent Desktop Displays, see “Upgrading the Agent Desktop Displays client software” on page 352.

Symposium Web Client and Remote Data Service

While the primary communication method in Symposium Web Client 4.5 is through SOAP 3.0, the application server still needs to use RDS communication in the following three instances:

- when Agent Desktop Displays 4.0 clients connect to the application server to view the displays

- during the upgrade process when you upgrade these clients to Agent Desktop Displays 4.5
- during the upgrade process when you upgrade all client PCs to SOAP 3.0

Until you have finished upgrading all client PCs to SOAP 3.0, and have upgraded all the client PCs running Agent Desktop Displays to Release 4.5 of the client software, the application server still requires that RDS be enabled (in addition to SOAP).

Since the RDS communication method relies on the MSADC virtual directory, this directory must also be enabled for proper RDS functionality, The default IIS Lockdown procedure, as documented in this guide, disables RDS by removing this virtual directory. However, when performing this procedure, you can choose to leave this directory enabled while there are still client PCs running Agent Desktop Displays 4.0 and connecting to the application server, and until you have upgraded all client PCs to SOAP 3.0.

For more information, see “Installing, configuring, and uninstalling IIS Lockdown and URLScan” on page 207.

Note: After you upgrade to Agent Desktop Displays Release 4.5, the first time you launch the program, the system checks for SOAP 3.0 on the client PC. If it does not find this software, then the system automatically downloads and installs the SOAP software. Since this process also requires RDS, you cannot remove the application server’s MSADC virtual directory through the IIS Lockdown procedure until the SOAP software has been completely installed on all client PCs that connect to the application server to view the Agent Desktop Displays.

Installing and configuring Agent Desktop Displays on a client PC

Note: For details on upgrading Agent Desktop Displays, see “Upgrading the Agent Desktop Displays client software” on page 352.

If the client operating system is Windows NT 4.0 Workstation, Windows XP, or Windows 2000, then you must be logged on to the PC with Administrator privileges to install Agent Desktop Displays. This also applies if you are installing the client portion of Agent Desktop Displays on the application server. The Windows 98 operating system does not require Administrator privileges.

- **Installing Agent Desktop Displays** To install Agent Desktop Displays on a client PC, run the setup program for the client version of the program. You must configure the agent displays on each client to connect to the application server, and to the server in Symposium Call Center Server after installation is complete.

ATTENTION

The Agent Desktop Displays 4.5 client software is incompatible with the Symposium Web Client 4.0 software that is installed on the application server. Once you upgrade the client PC from Agent Desktop Displays Release 4.0 to Release 4.5, then you cannot use the Agent Desktop Displays component when the client PC connects to an application server running Symposium Web Client 4.0.

Note: You can use this procedure to install both the standard English version and the multi-language support version of the Agent Desktop Displays client software. For more information on Agent Desktops Displays and multiple language support, see “Versions of ADD client software and multiple language support” on page 143.

To install and configure Agent Desktop Displays on a client PC

1 Insert the Symposium Web Client CD into the client PC.

2 Click Start → Run.

Result: The Run dialog box appears.

3 Click **Browse** to go to the CD-ROM drive on the client.

4 Open the **Agent Desktop Displays Client** folder, and then double-click the setup.exe file.

Example

Your path can be

[CD-ROM drive]:\Agent Desktop Displays Client\setup.exe

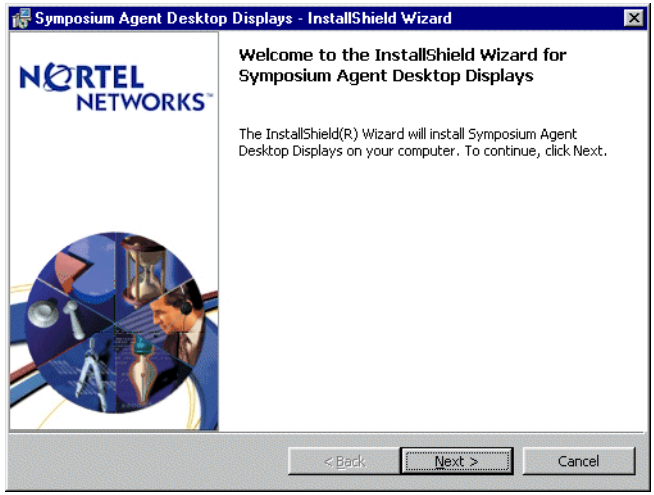
5 Click **OK**.

Result: The Choose Setup Language window appears.

6 From the drop-down list, choose the language in which you want to install/upgrade Agent Desktop Displays. You can choose from English, French, German, Japanese, and Traditional Chinese.

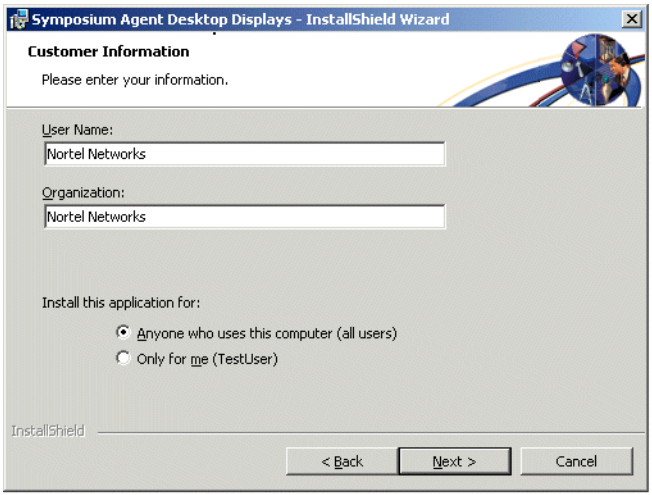
7 Click **OK**.

Result: The system prepares for setup and displays the Welcome to the InstallShield Wizard for Symposium Agent Desktop Displays window.



8 Click **Next**.

Result: The Customer Information window appears.



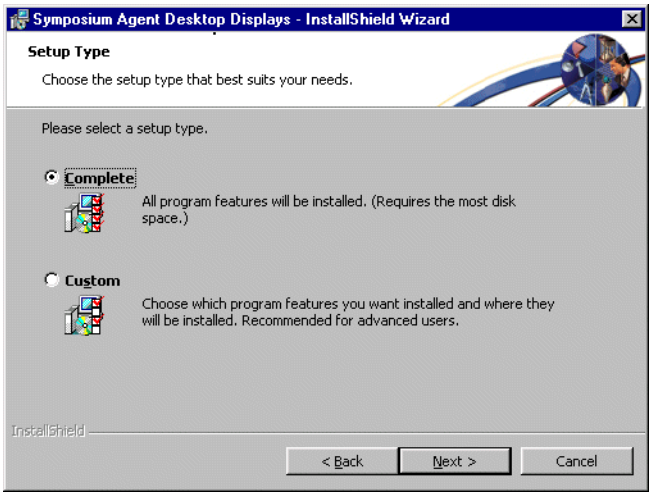
Note: This window is different on client PCs running Windows 98; the radio buttons under the heading **Install this application for** do not appear on these client PCs.

9 In the **User Name** and **Organization** boxes, type the appropriate information.

10 Under the **Install this application for** heading, click the radio button beside Anyone who uses this computer (all users).

11 Click **Next**.

Result: The Setup Type window appears.



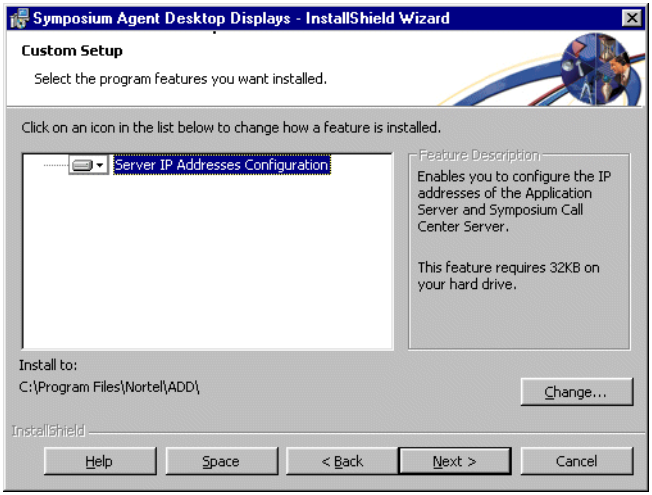
12 Select one of the following setup types:

- **Complete**: Click **Complete** to install all Agent Desktop Displays components in the default directory.
- **Custom**: Click **Custom** to select which Agent Desktop Displays components the system will install, to change to the default installation directory, or to confirm available hard disk space.

13 If you want to change the components to be installed, follow these steps:

a. Click **Custom** in the Setup Type window.

Result: The Custom Setup window appears.



b. Click the icon for the component that you do not want to install (for example, Tabular Display).

Result: A pop-up menu appears.

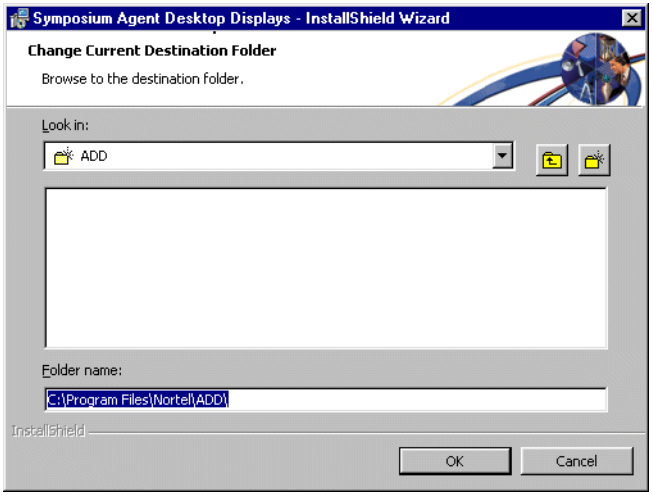
c. Click **This feature will not be available**.

Result: An X appears beside the name of the component.

14 Confirm the default directory path that appears in the bottom left side of the window. If you want to change the default directory path, follow these steps:

a. In the Custom Setup window, click **Change**.

Result: The Change Current Destination Folder window appears.



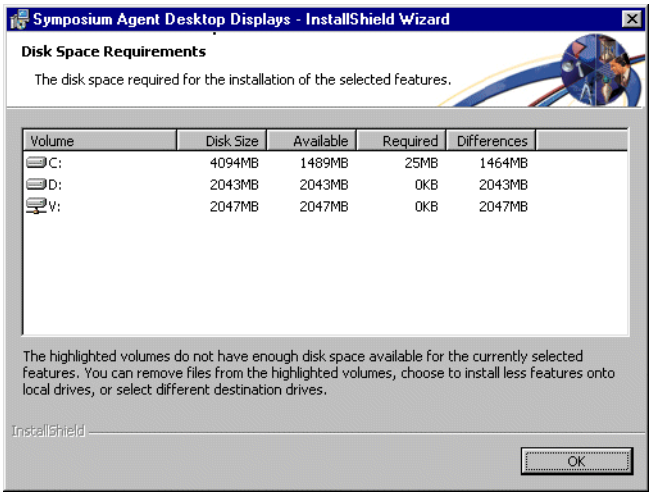
b. In the **Folder name** box, type the path to the directory and the directory name, or navigate to the drive and directory in which you want to install the program.

c. Click **OK** to return to the Custom Setup window.

Note: If you are upgrading from a previous version of Agent Desktop Displays, then you cannot choose the directory in which to install the software; you must install the upgrade in the same folder in which the original software is installed.

15 If you want to confirm your available hard disk space, click **Space**.

Result: The Disk Space Requirements window appears.

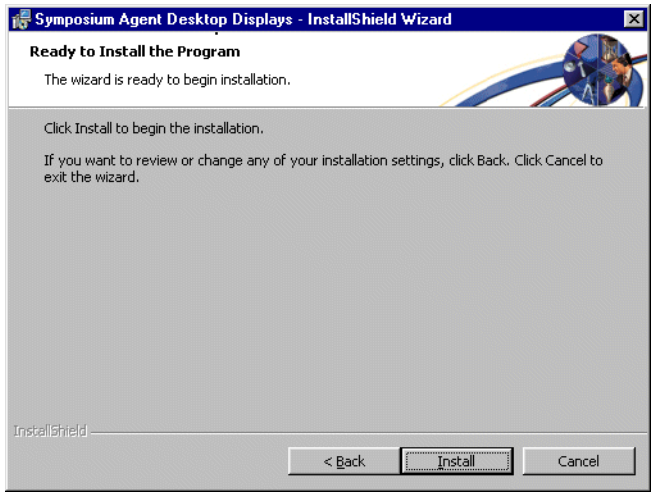


a. Review the available hard disk space and the amount of space required to install the individual components, and then click **OK** to return to the Custom Setup window.

Note: The Disk Space Requirements window appears automatically if you attempt to install Symposium Agent Desktop Displays on a drive that does not have enough free disk space.

16 Click **Next**.

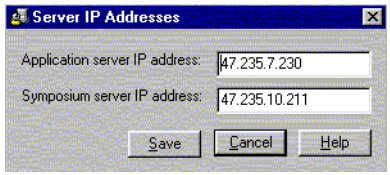
Result: The Ready to Install the Program window appears.



17 Click **Install**.

Note: If an application is running on the client whose files must be updated by the InstallShield, a Files in Use window appears. You must close any applications listed in this window, and then click **Retry**.

Result: The Installing Agent Desktop Displays window appears and installation begins. When installation is complete, the Server IP Addresses dialog box appears.



Note: If you are upgrading from a previous version of Agent Desktop Displays, then the Server IP Addresses window does not appear. Instead, the program uses the IP addresses that you originally chose. To change these addresses, after the client software is installed, use the Server IP Addresses window in the application.

18 In the **Application server IP address** and the **Symposium server IP address** boxes, type the appropriate IP addresses.

19 Click **Save**.

Result: The InstallShield Wizard Completed window appears.

20 Click **Finish**.

Result: The system may prompt you to restart your system.

Installing Simple Object Access Protocol on the Agent Desktop Displays client PC

Before you can use Agent Desktop Displays Release 4.5, the client PC must have the client SOAP software (clientSOAP.msi) installed. The system automatically downloads and installs the client SOAP software the first time a user launches Agent Desktop Displays.

Note: You must be logged on to the client PC with administrator privileges to complete the automatic downloading and installation of the client SOAP software.

The installation of the clientSOAP.msi file is required both on client PCs that are used to connect to the application server and work with Symposium Web Client (these PCs are most often designated for supervisors and administrators), and on client PCs that are used to run Agent Desktop Displays (these PCs are used by agents and some supervisors). However, the method of installing the SOAP software is slightly different in each case, as shown below:

- When you launch Symposium Web Client, the system checks whether SOAP 3.0 is installed. If it does not find the required files, it prompts you to download and install the SOAP software. You have three choices: you can click **Cancel** to download it later; you can save the software to the client PC's hard disk for later installation; or you can install the software immediately. You must be logged on to the PC with administrator privileges to install the software.
- When a user launches Agent Desktop Displays on a client PC, the system checks whether the client SOAP software (clientSOAP.msi) is installed. If it does not find the required files, then it *automatically* downloads the software. Once the download is complete, the system *automatically* installs the SOAP software. The user does not have the option of clicking **Cancel** or saving the installation file to disk for later installation. You must be logged on to the PC with administrator privileges to install the software. Once the installation process begins, the windows that appear are the same on both types of client PC. For details, see "To install Simple Object Access Protocol" on page 305.

Agent Desktop Displays and the MSADC folder

When you perform the optional IIS Lockdown procedure, it removes the MSADC virtual directory from the application server, which disables the RDS communication method.

Therefore, if you are using Agent Desktop Displays 4.0 with Symposium Web Client 4.5, you cannot perform the default IIS Lockdown procedure because the communication between the client PC and application server is through RDS, not SOAP. Instead, you can perform the IIS Lockdown procedure, but leave the MSADC virtual directory enabled. Once all Agent Desktop Displays clients have been upgraded to Release 4.5 (and have SOAP 3.0 installed), then you can perform the IIS Lockdown procedure again, this time removing the MSADC virtual directory. For more information on this procedure, see "Installing, configuring, and uninstalling IIS Lockdown and URLScan" on page 207.

Chapter 5

Upgrading Symposium Web Client

In this chapter

Overview 334

Pre-upgrade checklist 335

Upgrading Symposium Web Client 338

Upgrading the Agent Desktop Displays client software 352

Applying the latest Service Update 363

Overview

Introduction

This chapter is broken down into the following main subsections:

- **Pre-upgrade checklist** Use this checklist before you perform an upgrade to ensure that the server and client PCs are prepared properly.
- **Upgrading Symposium Web Client** This section includes the main procedures you must perform to upgrade Symposium Web Client from Release 4.0 to Release 4.5. These procedures include
  - upgrading the Sybase software from Release 12.0 to 12.5
  - upgrading the Symposium Web Client software

  For more information, see “Upgrading Symposium Web Client” on page 338.
- **Upgrading the Agent Desktop Displays client software** This section includes the procedures you must perform to upgrade the client PCs (and the application server if it is used as a client PC) to Release 4.5 of the Agent Desktop Displays client software. It includes the following procedures:
  - upgrading the Agent Desktop Displays software on the client PCs
  - upgrading the version of the client SOAP software installed on the client PCs
- **Applying the latest Service Update** This section includes the procedure you must perform to apply the latest Service Update to Symposium Web Client Release 4.5. For more information, see “Applying the latest Service Update” on page 363.

Pre-upgrade checklist

Introduction

Use this checklist before you upgrade Symposium Web Client from Release 4.0 to Release 4.5.

Pre-upgrade checklist

Note: Ensure that the conditions and prerequisites outlined in this checklist are met *before* you perform an upgrade.

General	✔
Check the latest installation or documentation addenda for updates. You can download the latest addendum from either http://www.nortelnetworks.com (for end customers), or http://www.nortelnetworks.com/prd/picinfo/ (for distributors).	❑
Ensure that you have the Symposium Web Client 4.5 installation CD-ROM on hand. Use this CD-ROM to upgrade the Symposium Web Client software to Release 4.5.	❑
Symposium Call Center Server	
Ensure that Symposium Call Center Server is running at least the following software release: ■ Symposium Web Client is compatible with either Symposium Call Center Server Release 4.0 (NS040107SU10S) or later, or Symposium Call Center Server Release 4.2 (NS040206SU08S) or later. Symposium Web Client is incompatible with previous releases of Symposium Call Center Server.	❑
Application server	
Before you upgrade Symposium Web Client from Release 4.0 to 4.5, ensure that you perform a full backup of the application server, including the operating system, the Symposium Web Client application software, the Symposium Web Client files that contain user data, Active Directory, and anything else that is specific to the server. For details, see “Overview” on page 146.	❑

Ensure that Sybase Open Client 12.5 is installed on the application server. For more information, see “Upgrading Sybase Open Client” on page 340.	❑
Ensure that the appropriate Sybase Open Client driver is installed. For details, see “To upgrade the Sybase 12.5 ODBC driver” on page 345.	❑
Before you upgrade Symposium Web Client from Release 4.0 to Release 4.5, ensure that the application server meets all minimum requirements for this Release. For details, see “Application server hardware requirements” on page 26, and “Application server software requirements” on page 27.	❑
If you have installed IIS Lockdown on the application server, you must uninstall it before upgrading Symposium Web Client Release 4.0 to Release 4.5, and then reinstall IIS Lockdown after the upgrade. For details, see “Installing, configuring, and uninstalling IIS Lockdown and URLScan” on page 207.	❑
If you are upgrading to a new release of Symposium Web Client, or adding additional features to your existing installation, ensure that you have the new key code. You must enter the new key code during the upgrade procedure. **Note:** If you are installing the latest Service Update, then you do not require a new key code.	❑
If you are upgrading the XML automated assignments feature, ensure that you have the *XML Assignments User Guide* on hand for instructions on installing and uninstalling this component. This guide, and other associated documentation and engineering/development support resources for the XML automated assignments feature, are provided only through the Nortel Networks Developer Program. For information on obtaining the XML Automated Assignment toolkit, contact a member of the Developer Program through the Contact Us link on their web site at http://www.nortelnetworks.com/developer.	❑
Client PCs	
Before you upgrade Symposium Web Client from Release 4.0 to Release 4.5, ensure that all client PCs meet the minimum requirements for this Release. For details, see “Client hardware requirements” on page 29, and “Client software requirements” on page 30.	❑

Before you upgrade the client PCs from Release 4.0 to 4.5 of the Agent Desktop Displays software, ensure that Remote Data Service (RDS) is installed and enabled on the application server. If you have removed the MSADC virtual directory by performing the IIS Lockdown procedure, then you have disabled RDS. To reenable it before upgrading Agent Desktop Displays, see “To reenable Remote Data Service” on page 244.	❑

Upgrading Symposium Web Client

Introduction

ATTENTION

Before you attempt a major upgrade of the Symposium Web Client application version, ensure that you have made a complete backup so that you can restore the entire Symposium Web Client application server should you need to do so. A complete backup of the Symposium Web Client application server includes the operating system, the Symposium Web Client application software, the Symposium Web Client files that contain user data, Active Directory, and anything else that is specific to the server.

Typically, you make a complete backup of the entire Symposium Web Client application server, including Active Directory, using a proven third-party backup tool of your choice, or the Windows 2000 Server backup method. When using the Windows 2000 Server backup method, select *System State* from the Backup tag. Refer to the Microsoft documentation for more details.

If you encounter a problem with the following upgrade process, or if you encounter a product problem, then you can use the full backup you created to revert to the previous version of Symposium Web Client. For more information see, “Overview” on page 146.

You can use the procedure in this section to

- upgrade the software to add additional features or components (for example, if you have purchased additional agent licenses, or if you want to add historical or real-time reporting capabilities)
- upgrade from Symposium Web Client Release 4.0 to Release 4.5

In each case, you enter your new keycode when you are prompted to do so during the installation.

Note: If you are upgrading from Symposium Web Client Release 4.0 to Release 4.5, then you must ensure that Sybase Open Client 12.5 is installed on the application server before you perform the upgrade. For more information, see "Upgrading Sybase Open Client" on page 340.

Service Updates

You can upgrade your Symposium Web Client software when new Service Updates or Releases become available. When you upgrade to a newer version of the software, you can download and apply the latest Service Update from https://www21.nortelnetworks.com/MPL (for Europe), or from https://www43.nortelnetworks.com/MPL (for North America). For more information on applying the latest Service Updates, see "Applying the latest Service Update" on page 363.

Note: If you are upgrading Symposium Web Client with the latest Service Update, then you do not require a keycode because the system upgrades only those components that were already installed on the application server.

You can download the latest installation or documentation addendum from either http://www.nortelnetworks.com (for end customers), or http://www.nortelnetworks.com/prd/picinfo/ (for distributors).

Main procedures in the upgrade

When you upgrade Symposium Web Client from Release 4.0 to 4.5, you must perform the following main procedures:

On the application server

1. Upgrade Sybase Open Client to v.12.5.
2. Upgrade the Sybase Open Client 12.5 ODBC driver, EBF11113.
3. Upgrade Symposium Web Client to Release 4.5.
4. If you have the client portion of Agent Desktop Displays installed on the application server, then you must upgrade this software too.

On the client PCs

5. Upgrade the Agent Desktop Displays software to Release 4.5.
6. Upgrade the client portion of the Simple Object Access Protocol (SOAP) software to version 3.0.

All these procedures are outlined in this section.

Upgrading Sybase Open Client

You must install Sybase Open Client v.12.5 to use the Historical Reporting and Contact Center Management components of Symposium Web Client 4.5. To install Sybase Open Client, you must have administrator privileges on the application server.

Note: If you have Sybase v.12.0 installed on the application server, then you can perform an upgrade to Sybase v.12.5 using the following procedure. If you have a version of Sybase earlier than 12.0 or later than 12.5 installed on the application server, then you must uninstall it before you install version 12.5. For information on uninstalling the software, see the documentation posted on the Sybase web site at http://manuals.sybase.com/onlinebooks/group-as/asp1200e/aseinsnt.

After you upgrade Sybase Open Client to version 12.5, you must upgrade the Sybase Open Client ODBC driver. For details, see “To upgrade the Sybase 12.5 ODBC driver” on page 345.

To upgrade Sybase Open Client

You can use this procedure to upgrade Sybase Open Client from v.12.0 to v.12.5. You must be logged on the server as an administrator to perform this procedure.

Symposium Web Client only functions with Sybase Open Client 12.5. If the application server already has a version of Sybase installed that is *newer* than version 12.5, then you must uninstall it completely before installing version 12.5. For information on uninstalling Sybase software, see the Sybase documentation. For information on performing a fresh installation of Sybase v.12.5 (as opposed to upgrading from v.12.0), see “To install Sybase Open Client” on page 89.

Tip: If the server already has Sybase Open Client installed, perform the following procedure to verify the version of the software:

a. On the server, Start → Settings → Control Panel.

b. Click **System**.

Result: The System Properties window appears.

c. Click the **Advanced** tab.

d. Click **Environment Variables**.

Result: The Environment Variables window appears.

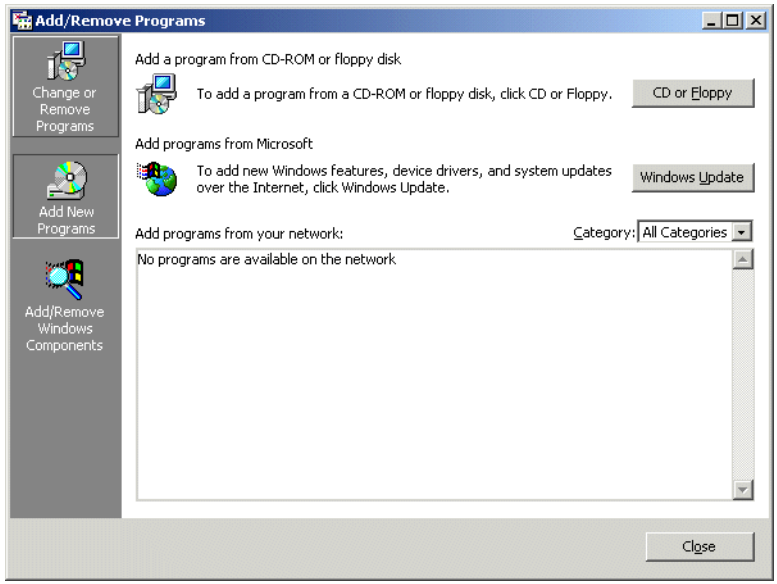
e. Within the System variables section, locate the Sybase software entries. For example, if Sybase Open Client Version 12.0 is installed on the server, it says *SYBASE_OCS: OCS_12_0*, and for Sybase Open Client Version 12.5, it says *SYBASE_OCS: OCS_12_5*.

1 On the application server, insert the Symposium Call Center Web Client CD in the CD-ROM drive.

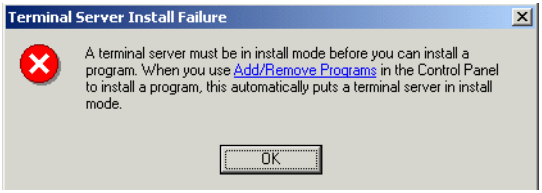
2 Click Start → Settings → Control Panel.

3 Double-click **Add/Remove Programs**.

Result: The Add/Remove Programs window appears.



Note: If you double-clicked the Sybase Open Client v.12.5 setup.exe file on the Symposium Web Client CD, or if the setup file launched automatically, the Terminal Server Install Failure dialog box appears. This occurs because Terminal Services must be in Install Mode before you can install an application.



To switch Terminal Services to Install Mode, select the Add/Remove Programs link in the dialog box. The Add/Remove Programs window appears, and Terminal Services automatically switches to Install Mode.

4 Click **Add New Programs**.

5 Click **CD or Floppy** to indicate that you want to install Sybase Open Client from the CD-ROM.

Result: The Install Program From Floppy Disk or CD-ROM window appears.

6 Click **Next**.

Result: The Run Installation Program window appears.

7 Click **Browse** and navigate to the Sybase folder on the CD-ROM: *D*:\SYBASE, where D:\ is the CD-ROM drive.

8 Double-click **setup.exe**.

Result: The path to the setup.exe file appears in the **Open** box.

9 Click **Next**.

Result: The Sybase Installer window appears, followed by the Installation Type window.

10 Click **Standard Install**, and then click **Next**.

Result: The Choose Directory window appears.

11 Nortel Networks recommends that when you are upgrading from Sybase 12.0, you choose the same folder in which the Sybase software is currently installed. However, if you do not know this location, then you can type a custom location in which to install the software, or accept the default path shown (C:\SYBASE).

ATTENTION

When choosing a custom location in which to install the Sybase software, do not choose a directory name that contains a space. For example, do *not* choose *D:\Program Files\Sybase* because the Sybase installation program cannot process the space in "Program Files."

12 Click **Next**.

Result: The Summary window appears, displaying the components being installed.

13 Click **Next**.

Result: The Create Directory window appears, prompting you to confirm the name of the directory to which the files will be copied.

14 Click **Yes**.

Result: The Installing window appears, displaying a status bar while the system installs the program. The system asks if you want to overwrite the following existing *Sybase* .DLL files. Click **Yes** when prompted to replace/ reinstall these Sybase files:

- replace mchelp.dll Version 12.0 with Version 12.5.0.0
- replace mclib.dll Version 12.0 with Version 12.5.0.0
- replace Language Modules version 12.0 with Version 12.5
- reinstall Component Sybase Central 3.2.0

If the system prompts you to replace the following optional file, you can click either **Yes** or **No**. Since the file is optional, your choice does not affect the Sybase installation:

- replace Power Dynamo Version 3.0.0 with Version 3.5.2

If the system prompts you to replace any other DLLs, including *system* DLLs, such as msvcrt40.dll Version 4.20, click **No**. Do not replace any system DLLs.

Note: If a window with the following message appears, click **OK**: *COMCTL32.DLL - The system does not need this update.*

When the installation is complete, the Sybase Installer window appears, prompting you to restart the system before configuring the installed components.

15 Click **Yes**.

Result: This can take several minutes. Do not attempt to manually restart the system. When restarting, log on as a user with administrator privileges. After the system restarts, the Information window appears, confirming the Sybase installation.

ATTENTION

Do not remove the Symposium Web Client CD from the CD-ROM drive during the system restart process. The Installation Wizard carries out some final configuration procedures after the system restarts.

16 Click **OK**.

17 Close the Control Panel window.

To upgrade the Sybase 12.5 ODBC driver

After you upgrade Sybase Open Client to Version 12.5, you must perform the following procedure to update the Sybase ODBC driver, EBF11113.

1. On the application server, free up all active Sybase Open Client connections as follows:
   a. Close all Symposium Web Client browser sessions.
   b. Stop any other third-party applications that are running on the application server and that use Sybase Open Client.
2. On the application server, reset IIS as follows:
   a. Click Start → Run.
   b. In the **Open** box, type *iisreset*, and then click **OK**.
3. Install the updated driver, EBF11113, as follows:
   a. On the application server, open an MS-DOS prompt, and then navigate to the root directory of the Symposium Web Client CD-ROM.
   b. Type the following xcopy command:

      copy EBF11113.* %SYBASE% /s /e /v /Y > C:\EBF11113.TXT*

      In this command, *EBF11113* is the directory containing the Sybase ODBC driver, *%SYBASE%* is the environment variable containing the directory location of Sybase Open Client 12.5 software installed on the application server, and *C:\EBF11113.TXT* is the log file that you can use to verify if all the files were copied correctly.
4. On the application server, verify that the system successfully updated the driver as follows:
   a. Click Start → Programs → Administrative Tools.
   b. Click the Data Sources (ODBC) icon.

      Result: The ODBC Data Source Administrator window appears.
   c. Click the **Drivers** tab.
   d. In the tab, scroll down until you locate the Sybase ASE ODBC driver. The correct driver version is 4.10.00.49.

Note: If the ODBC driver version is not 4.10.00.49, then open the log file, C:\EBF11113.txt, to verify if there were any error messages recorded during the xcopy.

What's next?

Upgrade Symposium Web Client to Release 4.5. For details, see "To upgrade Symposium Web Client" below.

To upgrade Symposium Web Client

Perform this procedure if you are upgrading Symposium Web Client from Release 4.0 to Release 4.5, or if you are upgrading the software to add additional features or components (for example, if you have purchased additional agent licenses, or if you want to add historical or real-time reporting capabilities). In both cases, you need a new key code.

Notes:

- Before performing this procedure, complete the pre-upgrade checklist on page 335.
- If you have installed IIS Lockdown on the application server, you must uninstall it before upgrading Symposium Web Client, and then reinstall IIS Lockdown after the upgrade. For details, see "To uninstall IIS Lockdown and reconfigure an application server that was installed as the default web site" on page 226 or "To uninstall IIS Lockdown and reconfigure an application server that was installed as part of an existing site" on page 234.
- You must be logged on to the application server as an administrator or as a user with administrator privileges before you can perform the following procedure.
- The application server must have Sybase Open Client 12.5 installed before you can upgrade Symposium Web Client. For more information on upgrading to this version of the Sybase software, see "Upgrading Sybase Open Client" on page 340.
- For information on reverting back to a previous version of Symposium Web Client after upgrading, see "Reverting back to a previous version of Symposium Web Client" on page 159.

1. Insert the Symposium Web Client installation CD into the application server.
2. Click Start → Settings → Control Panel.

3 Click the **Add/Remove Programs** icon.

Result: The Add/Remove Programs window appears.

4 Click **Add New Programs**.

5 Click **CD or Floppy**.

Result: The Install Program From Floppy Disk or CD-ROM window appears.

6 Click **Next**.

Result: The Run Installation Program window appears.

7 Click **Browse** to navigate to the *setup.exe* file located in the root directory of the CD, and then double-click the file.

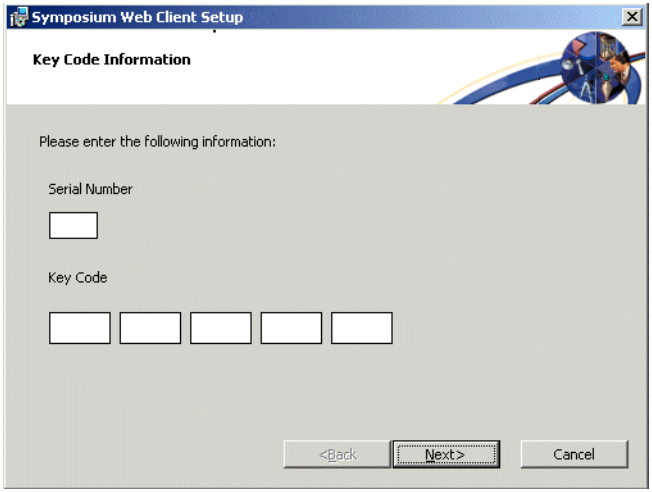
Result: The path and file name appear in the **Open** box.

8 Click **Next**.

Result: The Symposium Web Client Setup keycode upgrade window appears, asking if you want to change your keycode.

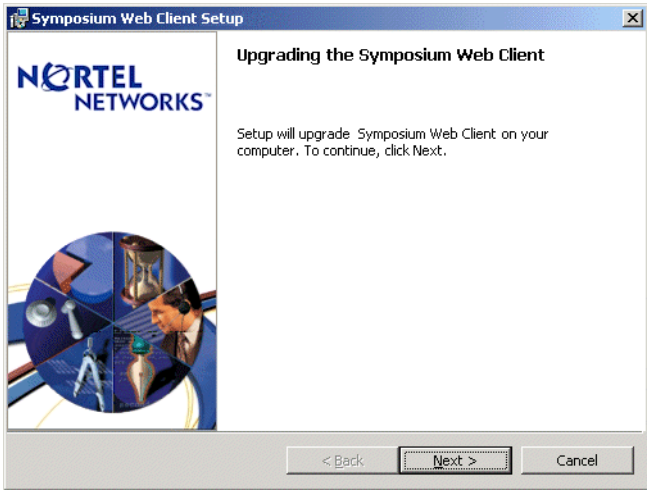
9 Click **Yes**.

Result: The Key Code Information window appears, prompting you to enter your new keycode.



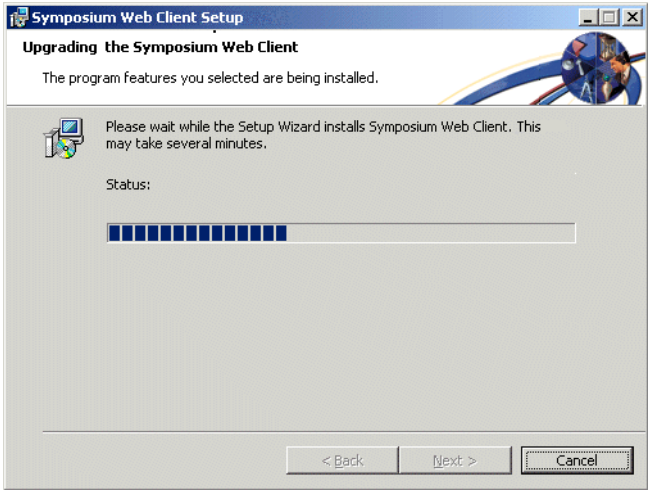
10 Type your new keycode, and then click **Next**.

Result: The Upgrading the Symposium Web Client main setup window appears.



11 Click **Next**.

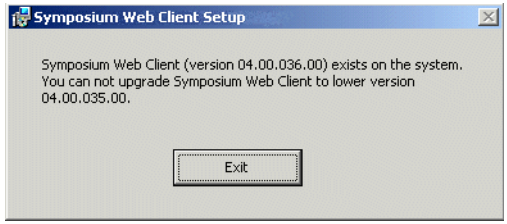
Result: The Upgrading the Symposium Web Client status window appears, and the system copies new files to the application server.



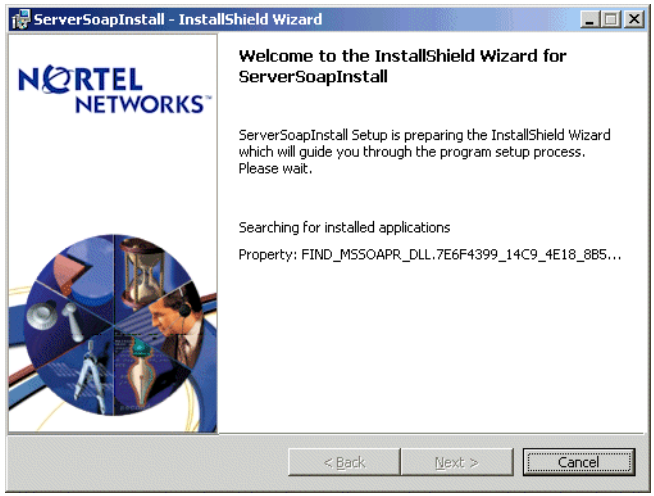
Notes:

- The Files in Use window appears if you have files open that the installation program needs to update. You must close the files shown in the window, and then click **Retry** to continue with the upgrade.

- You cannot upgrade to a previous version of Symposium Web Client. If you attempt to upgrade to a previous version, a message box appears, prompting you to end the upgrade process.



Once the system has copied the first series of installation files and the Crystal Reports templates, the Welcome to the InstallShield Wizard for ServerSOAPInstall window appears.



Note: Sometimes the above window does not appear; instead, the system automatically starts installing the SOAP files. In this case, proceed to the next step.

12 The program searches for installed components, and then installs the required SOAP files. When it is finished, the Completing the Symposium Web Client Setup Wizard window appears.

13 Click **Finish**.

Result: The Symposium Web Client Installer Information window appears, indicating that you must restart the application server for the upgrade to take effect.

14 Click **Yes**.

What's next?

After you finish upgrading Symposium Web Client on the application server, check the following:

- If you have the client portion of Agent Desktop Displays installed on the application server, then you will also need to upgrade this software on the server, in addition to the client PCs. For more information, see "Upgrading the Agent Desktop Displays client software" on page 352.
- If you want to be able to use the unicast data transmission method for your real-time displays, then you must configure Real-Time Reporting to allow this type of transmission (the default transmission type is multicast only). For more information, see "To configure Real-Time Reporting" on page 167.
- If you have installed the XML automated assignments feature, then you must upgrade it by uninstalling the existing version of the software and reinstalling the new version. For details on uninstalling and installing this software, see the *XML Assignments User Guide*. This guide, and other associated documentation and engineering/development support resources for the XML automated assignments feature, are provided only through the Nortel Networks Developer Program. For information on obtaining the XML Automated Assignment toolkit, contact a member of the Developer Program through the Contact Us link on their web site at http://www.nortelnetworks.com/developer. General information on the Developer Program, including an online membership application, is also available on this site.
- Ensure that all client PCs connecting to the upgraded application server have the required software. For more information, see Chapter 4, "Installing and configuring client software."
- Perform a test on the application server to ensure that the upgrade was successful. For example, verify that your existing historical reports and real-time displays are still present and function correctly.

Upgrading the Agent Desktop Displays client software

Introduction

You can use the procedure in this section to upgrade the Agent Desktop Displays client software that is installed on the application server (when the server is also used as a client) and on the client PCs.

Agent Desktop Displays Release 4.0 is compatible with an application server running Release 4.5. However, when you use a client PC running Agent Desktop Displays Release 4.0 to connect to an application server running Symposium Web Client Release 4.5, a message appears, notifying you that there is a newer version of the client software available and enabling you to automatically upgrade the software to Release 4.5. This message box also appears if you are using the client portion of Agent Desktop Displays 4.0 when it is installed on an application server that is running the Symposium Web Client 4.5 server software.

If you choose to upgrade, then the installation program automatically begins to upgrade and install the software. If you choose not to upgrade, then you can continue to use Agent Desktop Displays Release 4.0. However, in this case, the communication between the client PC and application server continues to be through Remote Data Service (RDS), rather than SOAP, which is new to Release 4.5. Therefore, the RDS communication method must be enabled on the application server for Agent Desktop Displays 4.0 to function properly.

For more information on Agent Desktop Displays, see “Installing and configuring Agent Desktop Displays on a client PC” on page 320.

Symposium Web Client and Remote Data Service

The RDS communication method is enabled by default on the application server. However, if you have performed the IIS Lockdown procedure on the application server and you have removed the MSADC virtual directory, then you have disabled RDS. For details on reenabling RDS, see “To reenable Remote Data Service” on page 244.

After you upgrade to Agent Desktop Displays Release 4.5, the first time you launch the program, the system checks for SOAP 3.0 on the client PC. If it does not find this software, then the system automatically downloads and installs the SOAP software. Since this process also requires RDS, you cannot remove the application server's MSADC virtual directory through the IIS Lockdown procedure until the SOAP software has been completely installed on all client PCs that connect to the application server to view the Agent Desktop Displays. For more information, see "Installing Simple Object Access Protocol on the Agent Desktop Displays client PC" on page 359.

In summary, while the primary communication method in Symposium Web Client 4.5 is through SOAP 3.0, the application server still needs to use RDS communication in the following three instances:

- when Agent Desktop Displays 4.0 clients connect to the application server to view the displays
- during the upgrade process when you upgrade these clients to Agent Desktop Displays 4.5
- during the upgrade process when you upgrade all client PCs to SOAP 3.0

Therefore, until you have finished upgrading all client PCs to SOAP 3.0, and have upgraded all the client PCs running Agent Desktop Displays to Release 4.5 of the client software, the application server still requires that RDS be enabled (in addition to SOAP).

You have two options:

- If you have already disabled RDS by performing the IIS Lockdown procedure, then you must reenable it. For details, see "To reenable Remote Data Service" on page 244.
- You can perform the IIS Lockdown procedure, but leave the MSADC virtual directory enabled. Once all Agent Desktop Displays clients have been upgraded to Release 4.5 (and have SOAP 3.0 installed), then you can perform the IIS Lockdown procedure again, this time removing the MSADC virtual directory. For more information on this procedure, see "Installing, configuring, and uninstalling IIS Lockdown and URLScan" on page 207.

Upgrading Agent Desktop Displays and the MSADC folder

You only need to perform the procedure in this section, "To set the permissions on the MSADC folder before upgrading Agent Desktop Displays to Release 4.5" on page 355, if the following conditions exist:

- You have completed a *fresh* installation of the Symposium Web Client Release 4.5 software on the application server (you have not upgraded the application server software from a previous release).
- You are performing an automatic upgrade of your Agent Desktop Displays client software from Release 4.0 to Release 4.5 by connecting to this application server.

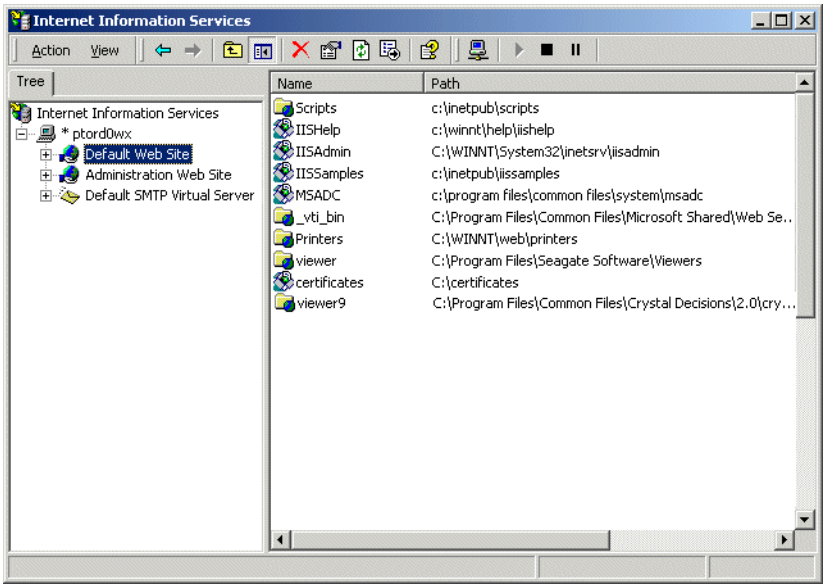
If these conditions do not apply to you (for example, if you have *upgraded* the application server software to Release 4.5), then you do not need to perform this procedure because the permissions on the MSADC folder are already set properly. Instead, you can proceed directly with upgrading Agent Desktop Displays. For details, see "To upgrade the Agent Desktop Displays client software" on page 356.

When you install IIS on the application server, the security permissions for the MSADC virtual directory are automatically set to *Denied Access*, which prevents the automatic upgrade of Agent Desktop Displays 4.0 clients to Agent Desktop Displays 4.5. To enable the automatic upgrade to proceed, you must first set the permissions on this folder to *Granted Access*, according to the following procedure.

To set the permissions on the MSADC folder before upgrading Agent Desktop Displays to Release 4.5

1 On the application server, click Start → Programs → Administrative Tools → Internet Services Manager.

Result: The Internet Information Services window appears.



2 In the left pane, double-click the server name.

Result: The heading expands to reveal a series of folders.

3 Double-click **Default Web Site**.

Result: The heading expands to reveal a new series of folders.

4 Right-click the MSADC virtual folder, and from the resulting pop-up menu, click **Properties**.

Result: The MSADC Properties window appears.

5 Click the **Directory Security** tab.

6 Under the **IP address and domain name restrictions heading**, click **Edit**.

Result: The IP Address and Domain Name Restrictions window appears.

7 Click the radio button beside **Granted Access**, and then click **OK**.

8 Click **OK** to close the MSADC Properties window and save your changes.

9 Close the Internet Information Services window.

Result: You can now proceed with the automatic upgrade of Agent Desktop Displays from Release 4.0 to Release 4.5. For more information, see "To upgrade the Agent Desktop Displays client software" below.

To upgrade the Agent Desktop Displays client software

Notes:

- Before you can successfully perform this automatic upgrade, you must ensure that the MSADC virtual folder on the application server has the proper permissions. For more information, see "To set the permissions on the MSADC folder before upgrading Agent Desktop Displays to Release 4.5" on page 355.
- If the client operating system is Windows NT 4.0 Workstation, Windows XP, or Windows 2000, then you must be logged on to the PC with Administrator privileges to upgrade Agent Desktop Displays. This also applies if you are upgrading the client portion of Agent Desktop Displays on the application server. The Windows 98 operating system does not require Administrator privileges.

ATTENTION

The Agent Desktop Displays 4.5 client software is incompatible with the Symposium Web Client 4.0 software that is installed on the application server. Once you upgrade the client PC from Agent Desktop Displays Release 4.0 to Release 4.5, then you cannot use the Agent Desktop Displays component when the client PC connects to an application server running Symposium Web Client 4.0.

1 Log on to the client PC (or the application server, if it has the client portion of Agent Desktop Display installed) with Administrator privileges (all PCs except those running Windows 98).

2 On the client PC, open Agent Desktop Displays and connect to an application server running Symposium Web Client 4.5.

3 Launch a tabular display.

Result: A message box appears, asking if you want to upgrade to a newer version of Agent Desktop Displays.

4 Click **Yes**.

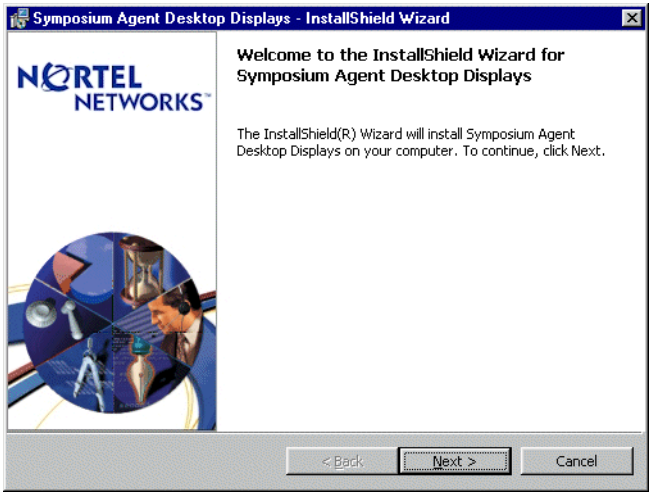
Result: The Choose Setup Language window appears.

5 From the drop-down list, choose the language in which you want to upgrade Agent Desktop Displays. You can choose from English, French, German, Japanese, and Traditional Chinese.

Note: For more information on Agent Desktops Displays and multiple language support, see “Versions of ADD client software and multiple language support” on page 143.

6 Click **OK**.

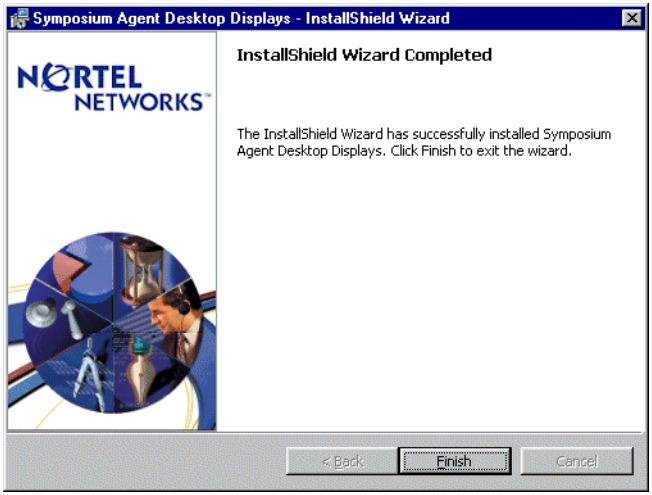
Result: The system prepares for setup and displays the Welcome to the InstallShield Wizard for Symposium Agent Desktop Displays window.



7 Click **Next**.

Note: If an application is running on the client whose files must be updated by the InstallShield, a Files in Use window appears. You must close any applications listed in this window and click **Retry**.

Result: The system copies the necessary files, and then installation begins. When you are upgrading from a previous version of Agent Desktop Displays, you cannot change the server IP addresses during the upgrade. Instead, the program uses the IP addresses that you originally chose. To change these addresses, after the client software is installed, use the Server IP Addresses window in the application. When the upgrade is complete, the InstallShield Wizard Completed window appears.



8 Click **Finish**.

Result: The system may prompt you to restart your system.

What's next?

Install the SOAP 3.0 client software on all client PCs, including the application server if it is used as a client PC. For details, see "Installing Simple Object Access Protocol on the Agent Desktop Displays client PC" on page 359.

Installing Simple Object Access Protocol on the Agent Desktop Displays client PC

Before you can use Agent Desktop Displays Release 4.5, the client PC must have the client SOAP software (clientSOAP.msi) installed. When a user launches Agent Desktop Displays 4.5 on a client PC, the system checks whether the client SOAP software (clientSOAP.msi) is installed. If it does not find the required files, then it *automatically* downloads the software. Once the download is complete, the system *automatically* installs the SOAP software.

When installing SOAP on the Agent Desktop Displays client, you do not have the option of saving the installation file to disk for later installation. Instead, you must be logged on as administrator to complete the automatic download and installation. If you are not logged on as a user with administrator privileges, then you can click **Cancel** to stop the installation. However, you cannot use Agent Desktop Displays 4.5 until you successfully download and install the client SOAP software.

To install Simple Object Access Protocol on the Agent Desktop Displays client PC

Notes:

- You must be logged on to the client PC with administrator privileges to complete the automatic downloading and installation of the client SOAP software.
- The client PC must have the Windows Installer 2.0 installed before you can perform this procedure. You can install the software from the Symposium Web Client CD-ROM. For more information, see “To install Windows Installer 2.0 or later” on page 101. After you update the Windows Installer, you must restart the PC.
- You only need to perform the SOAP installation once on each client PC, regardless of the number of Symposium Web Client upgrades you install afterward.

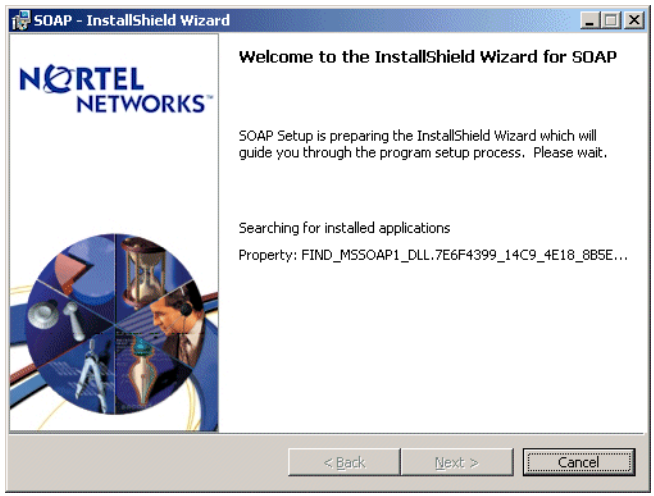
1 On the client PC, open Agent Desktop Displays 4.5 and connect to the application server.

2 Launch the tabular display.

Result: The installation program verifies the operating system and setup of the client PC and notifies you if you need to update the Windows Installer software.

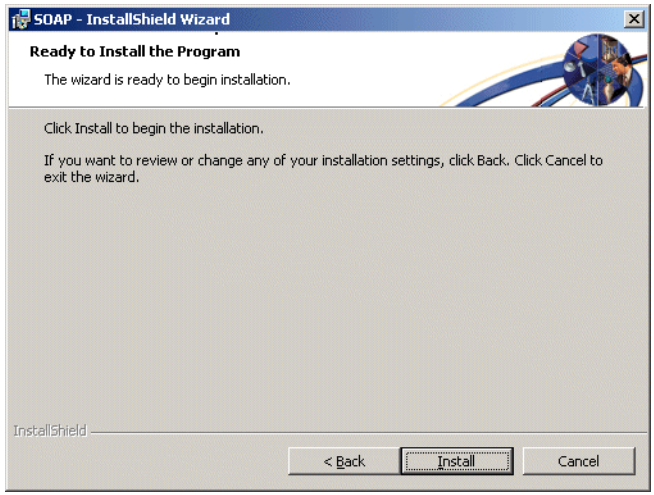
- If you need to update the Windows Installer package, you can install the software from the Symposium Web Client CD-ROM. For more information, see “To install Windows Installer 2.0 or later” on page 101. After you update the Windows Installer, you must restart the PC.
- If you do not have to update the installer, proceed to the following step.

3 The SOAP installation proceeds and the welcome window appears. You may have to wait a few moments while the program searches for installed applications, as shown in the following graphic:



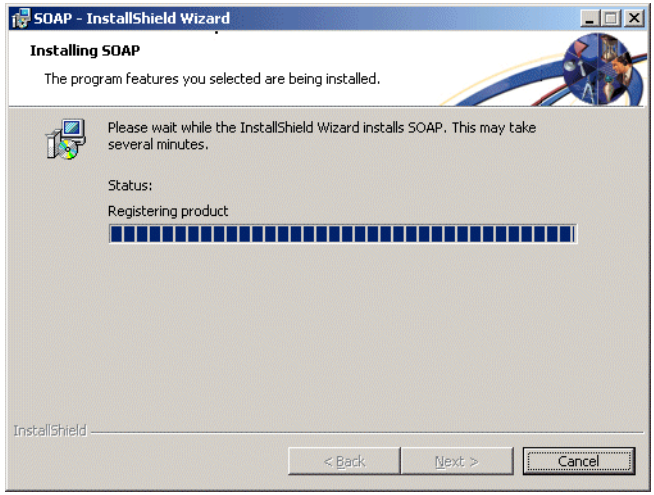
4 When the program finds the required applications, click **Next**.

Result: The Ready to Install the Program window appears.



5 Click **Install**.

Result: The Installing SOAP window appears.



6 The program installs the required SOAP components. When it is finished, the InstallShield Wizard Completed window appears.

7 Click **Finish.**

Result: You can now use Agent Desktop Displays 4.5.

Applying the latest Service Update

Introduction

This section includes the steps you must perform to apply the latest Service Update for Symposium Web Client 4.5. After you have successfully upgraded to the latest release of the software, you can download and apply the latest Service Update from https://www21.nortelnetworks.com/MPL (for Europe), or from https://www43.nortelnetworks.com/MPL (for North America).

Note: To register for either of these web sites, follow the instructions listed at http://nortelnetworks.com/register.

Once you download the Service Update from either of the sites listed above, you can perform the procedure in this section to install the Service Update on the application server. This procedure is very similar to that for performing an upgrade from one release to another, with the following exceptions:

- You do not need to upgrade Sybase Open Client again; you only need to upgrade the Sybase software once (before performing the Symposium Web Client upgrade from Release 4.0 to 4.5).
- You do not need to enter a new key code.

After you install the Service Update, if you encounter problems, you may need to revert back to the previous version of Symposium Web Client. For more information, see “Overview” on page 146.

To apply the latest Service Update

Note: You must be logged on to the application server as an administrator or as a user with administrator privileges before you can perform the following procedure.

1 On the Symposium Web Client 4.5 application server, navigate to the appropriate web site for downloading the latest Service Update (either https://www21.nortelnetworks.com/MPL [for Europe], or https://www43.nortelnetworks.com/MPL [for North America]).

Note: To register for either of these web sites, follow the instructions listed at http://nortelnetworks.com/register.

2 Download the latest Service Update and save it on the application server.

3 Click Start → Settings → Control Panel.

4 Click the **Add/Remove Programs** icon.

Result: The Add/Remove Programs window appears.

5 Click **Add New Programs**.

6 Click **CD or Floppy**.

Result: The Install Program From Floppy Disk or CD-ROM window appears.

7 Click **Next**.

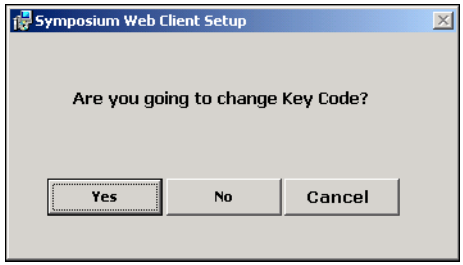
Result: The Run Installation Program window appears.

8 Click **Browse** to navigate to the *setup.exe* file for the Service Update that you downloaded, and then double-click the file.

Result: The path and file name appear in the **Open** box.

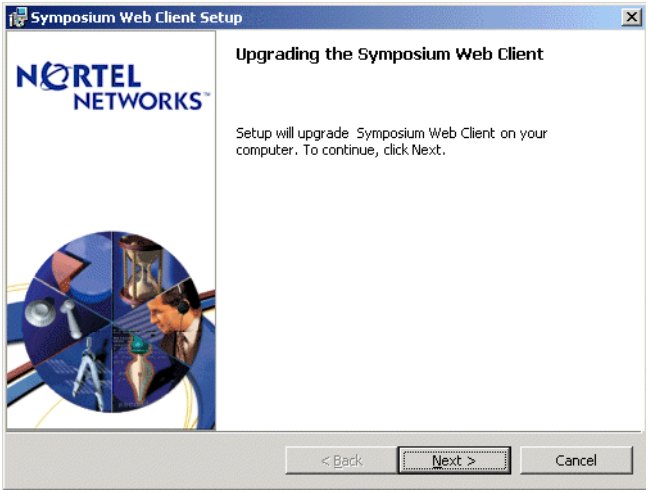
9 Click **Next**.

Result: The Symposium Web Client Setup keycode upgrade window appears, asking if you want to change your keycode.



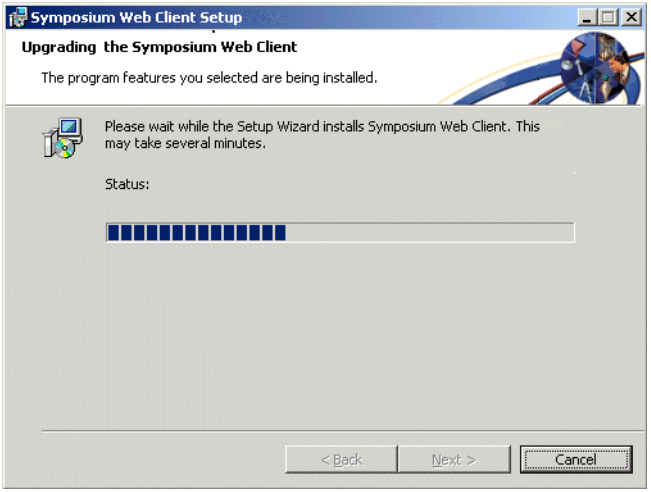
10 Click **No**.

Result: The Upgrading the Symposium Web Client main setup window appears.



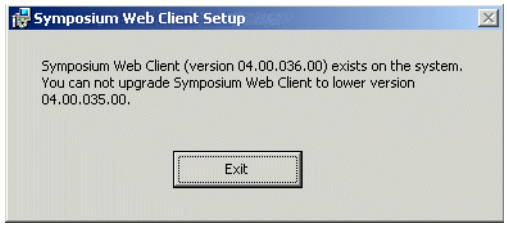
11 Click **Next**.

Result: The Upgrading the Symposium Web Client status window appears, and the system copies new files to the application server.

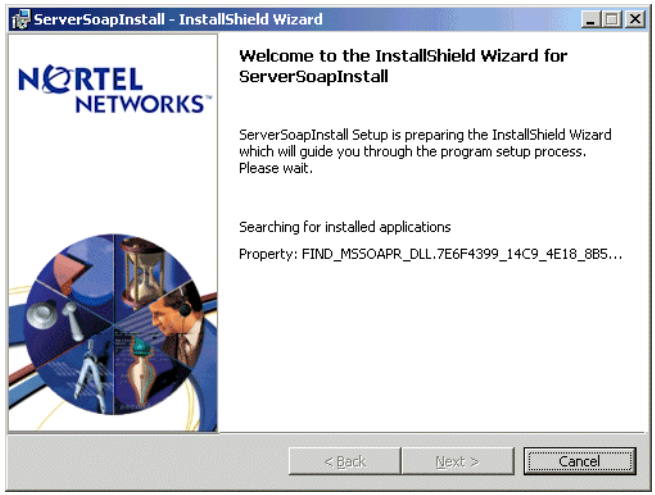


Notes:

- The Files in Use window appears if you have files open that the installation program needs to update. You must close the files shown in the window, and then click **Retry** to continue with the upgrade.
- You cannot upgrade to a previous version of Symposium Web Client. If you attempt to upgrade to a previous version, a message box appears, prompting you to end the upgrade process.



Once the system has copied the first series of installation files and the Crystal Reports templates, the Welcome to the InstallShield Wizard for ServerSOAPInstall window appears.



Note: Sometimes the above window does not appear; instead, the system automatically starts installing the SOAP files. In this case, proceed to the next step.

12 The program searches for installed components, and then installs the required SOAP files. When it is finished, the Completing the Symposium Web Client Setup Wizard window appears.

13 Click **Finish**.

Result: The Symposium Web Client Installer Information window appears, indicating that you must restart the application server for the upgrade to take effect.

14 Click **Yes**.

Chapter 6

Using Symposium Web Client

In this chapter

Overview 370

Section A: Getting started with Symposium Web Client 373

Section B: Configuration 383

Section C: Contact Center Management 401

Section D: Access and Partition Management 435

Section E: Audit Trail 481

Section F: Scripting 487

Overview

Introduction

Symposium Web Client is a browser-based tool designed to facilitate the management of call centers and their users.

Symposium Web Client components

Symposium Web Client consists of the following components:

Contact Center Management

Contact Center Management allows you to add, edit, view, or delete users on a server in Symposium Call Center Server, agent to supervisor assignments, and agent to skillset assignments. Users with the appropriate access class can also assign agents and supervisor/agents to partitions in this component.

Access and Partition Management

With this component, you can add, edit, view, or delete Web Client users, partitions, access classes, and report groups. You can also assign partitions, access classes, basic access rights, and supervisors and their reporting agents to users.

Configuration

The Configuration component is designed to assist the call center administrator in configuring and administering Symposium Call Center Server. Administrators using the Configuration component must be logged on as *webadmin* to add and configure servers, and to upload and download data using the Symposium Configuration spreadsheets.

Scripting

The Scripting component assists call center administrators in developing custom routing instructions for their call center. Scripting provides a graphical user interface for easy variable creation and access to a list of scripting commands that can be used when creating scripts.

Real-Time Reporting

Designed for call center supervisors, Real-Time Reporting allows you to view the dynamics of call activity. Real-time displays are available for both networked and single sites. This is an optional component.

Historical Reporting

You can generate summarized historical reports that contain totals for information gathered during a specific interval of time, and Event/detail reports for specific events that have occurred in the call center. This is an optional component.

Emergency Help

Agents can press the Emergency key when they require assistance from the supervisor (for example, if the caller is abusive). When a supervisor opens the Emergency Help panel, the system notifies the supervisor automatically whenever an agent presses the Emergency key on his or her phoneset. The Emergency Help panel shows information about the agent, including the agent's name, location, and time when the Emergency key was pressed.

Audit Trail

Audit Trail records the actions performed in the Configuration component, and identifies the user ID of the person who made the changes.

Agent Desktop Displays

Symposium Agent Desktop Displays provides real-time skillset monitoring to agents. Agent Desktop Displays must be configured on the application server, and on client PCs that use the tool.

The role of the administrator

This chapter is intended for administrators and provides conceptual information about the components that administrators use to configure a call center:

- Configuration
- Contact Center Management (administrative functions)
- Access and Partition Management
- Audit Trail
- Scripting

For conceptual information about Real-Time Reporting, Historical Reporting, Contact Center Management (supervisor functions) and Emergency Help, refer to the *Symposium Call Center Web Client Supervisor's Reference Guide.* For detailed procedures, refer to the online Help.

To find out more about using a component

For information on the boxes, buttons, and procedures for using any of the components in Symposium Web Client, open the component that you want to use, and then click Help → On This Window. Help for the current window appears. Click the Procedures book in the online Help's table of contents to view a list of Symposium Web Client procedures.

To view Help procedures specific to one component, click the component name in the table of contents, and then review the topics listed for that component.

Section A: Getting started with Symposium Web Client

In this section

Overview 374
High-level task flow 375
Starting Symposium Web Client 378

Overview

Introduction

Once you have installed and configured Symposium Web Client and any required third-party applications on the application server and the client PCs, you can begin using the application.

This section provides you with the following information:

- high-level task flow
- procedures for logging on to Symposium Web Client

High-level task flow

The following task flow provides a high-level overview of the steps you must perform to configure your call center using Symposium Web Client.

	Perform this step	in this component
1	Add each Symposium Call Center Server in the network. **Note:** Before you can add a newly configured server in Symposium Call Center Server, you must first change the server's default password. Since Symposium Web Client does not allow you to change this password in the Configuration component, you must use the Symposium Call Center Server client to log on to brand new servers for the first time. Once you change the default password, you can then use Symposium Web Client to add the desired servers.	■ Configuration
2	Upload Symposium Call Center Server configuration resources for each server. OR	■ Configuration
3	Configure each server by adding the resources, such as skillsets, CDNs, DNISs, and threshold classes individually. **Note:** Administrators must be logged on as *webadmin* to add and configure servers, and to upload and download configuration data.	■ Configuration

	Perform this step	in this component
4	Upload Symposium Call Center Server user data. OR	■ Configuration
5	Create individual Symposium Call Center Server users.	■ Contact Center Management
6	Designate the users as supervisors, agents, or supervisor/agents, and assign agents to the supervisors.	■ Configuration or Contact Center Management
7	Create any custom report groups that Web Client users require.	■ Access and Partition Management → Report Groups
8	Define the access classes that Web Client users require.	■ Access and Partition Management → Access Classes
9	Create the appropriate partitions for the call center, specifying the agents, applications, skillsets, CDNs, DNISs, and report groups that belong in each partition. **Note:** All agents that are assigned to a supervisor must also be included in the supervisor's partition so that the supervisor can monitor the agents in Real-Time Reporting, Historical Reporting, and Contact Center Management. The exception to this is if you also assign the user a supervisor/reporting agent combination. If you assign *both* a partition (even one containing no agents) *and* a supervisor/reporting agent combination to a user, then the user sees all his or her agents.	■ Access and Partition Management → Partitions

	Perform this step	in this component
10	Create the Web Client users. Grant each user basic access rights to specific Symposium Web Client components, and assign the appropriate partitions, access classes, and supervisors and their reporting agents to each user.	■ Access and Partition Management → Users

Starting Symposium Web Client

Introduction

Before you log on to Symposium Web Client, make sure you have installed all required third-party applications on the client PC, including Internet Explorer 5.5 Service Pack 2 (or later) and SOAP 3.0. You must also configure your browser appropriately. See “Installing third-party software on a client” on page 288 for more information.

To log on to Symposium Web Client for the first time

When you log on to Symposium Web Client for the first time after installation, you must log on as the default administrator, *webadmin*. For security reasons, it is highly recommended that you change the default password when you first log on to the application. Symposium Web Client user passwords can only contain English characters.

To log on to the application server for the first time and change the default password

ATTENTION

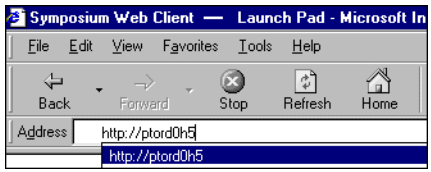
When you change the *webadmin* password, you must ensure that you do not lose or forget the new password or you cannot log on to Symposium Web Client as the *webadmin* administrator. In this case, you must uninstall and reinstall Symposium Web Client to reinstate the original *webadmin* user account with the default password.

Tip: To avoid this scenario, immediately after installing Symposium Web Client, log on to the application server as *webadmin* and create a new administrator account of your choice (for example, *tempadmin*), giving this user account Access and Partition Management rights. This way, if you lose or forget your new *webadmin* password, you can still log on to the application server as *tempadmin* and change the *webadmin* password. For more information on adding Web Client users, see the online Help.

1 Start Internet Explorer.

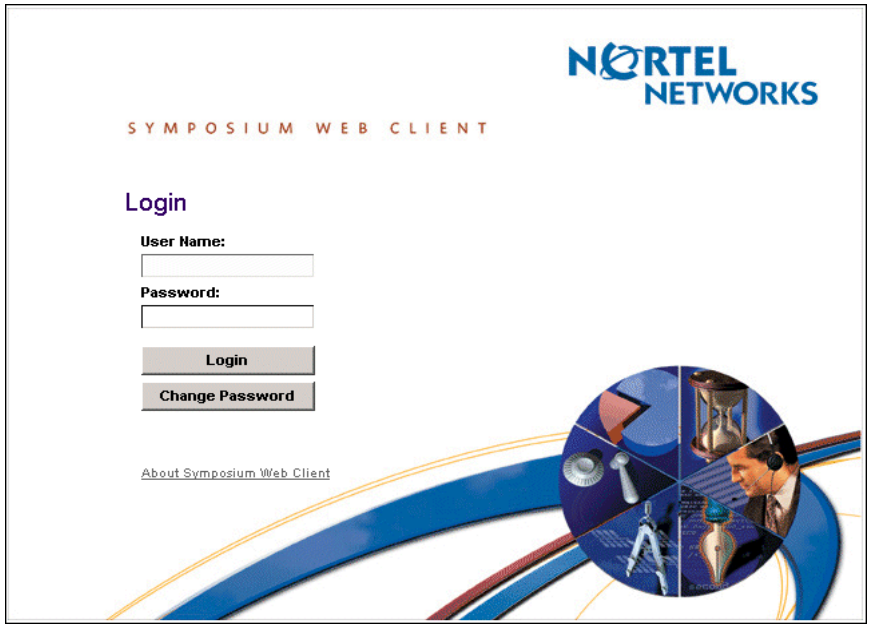
2 In the Address box, type the URL address of the application server. The default URL address is http://<*Application Server*>.

Note: Do not type the IP address of the application server. If you type the IP address instead of the URL, you may experience problems while working in the Scripting component.



Tip: You can save the application server's address by adding it to your list of Internet Explorer Favorites.

Result: The application server displays the Symposium Web Client main logon window.



Note: Click **About Symposium Web Client** to view a dialog box containing details of the Symposium Web Client build number and Service Update version.

3 Click **Change Password**.

4 Enter the default password.

5 Enter a new password.

Note: Symposium Web Client user passwords can only contain English characters.

6 Reenter the new password.

Note: You can modify only the default user name's password. The default user name *webadmin* cannot be changed.

7 Click **Submit**.

Result: The default password is changed and the main logon window reappears.

8 In the main logon window, type the user name and the password, and then click **Login**.

Result: If you have not installed the client version of SOAP 3.0 on the PC, a warning message appears, notifying you that you must install this software. For details on installing it, see “Viewing the list of installed third-party controls” on page 319. If you have already installed this software, then the main application window appears.

Tip: If you lose or forget the new *webadmin* password, you cannot log on to Symposium Web Client as the *webadmin* administrator. In this case, you must uninstall and reinstall Symposium Web Client to reinstate the original *webadmin* user account with the default password. To avoid this scenario, as a safety precaution, you can now open Access and Partition Management and create a new user account with administrator rights, such as *tempadmin*. If ever you forget or lose the new *webadmin* password you entered, you can log on to the application server as *tempadmin* and change the *webadmin* password.

Default time-out rate

Symposium Web Client no longer has a default time-out rate. Your session will not time out if the application remains idle.

What's next?

After you have logged on to the application server for the first time, you must add and configure the servers in Symposium Call Center Server using the Configuration component. Only administrators who are logged on as *webadmin* can add and configure servers in Symposium Call Center Server.

Refer to the "High-level task flow" on page 375 for a configuration overview, or refer to "Configuration" on page 383 for conceptual information.

For detailed step-by-step procedures, refer to the online Help in the Configuration component.

Section B: Configuration

In this section

Overview	384
Adding and configuring call center servers	386
Configuring resources	391

Overview

Configuration component

There are two main tasks that you perform using the Configuration component:

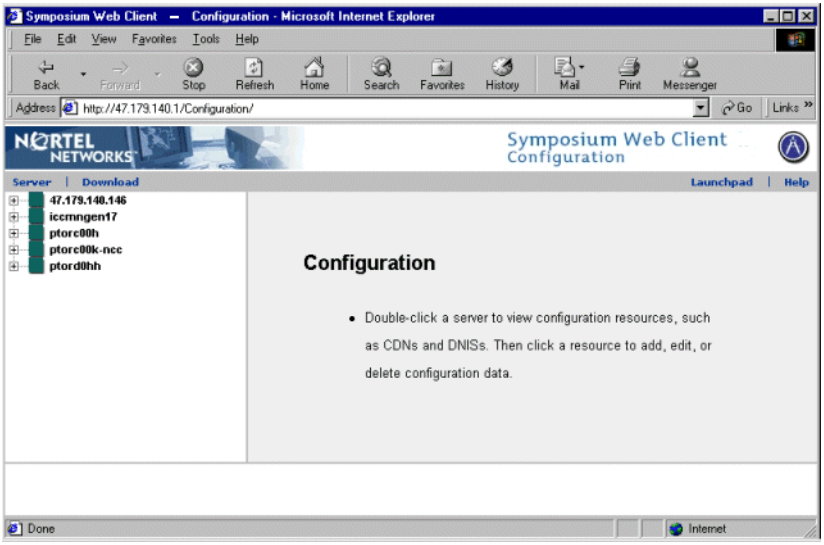
- adding, configuring, and deleting servers in Symposium Call Center Server
- adding, configuring, and deleting resources
  - individually using the web-based user interface

    or
  - uploading and downloading bulk data using the Configuration spreadsheets

Note: You must be logged on to Symposium Web Client as *webadmin* to add and configure servers, and to upload and download data using the Symposium Configuration spreadsheets.

This chapter provides a high-level overview of these procedures. For step-by-step procedures about using the Configuration component, see the Symposium Web Client online Help.

Configuration main window



Adding and configuring call center servers

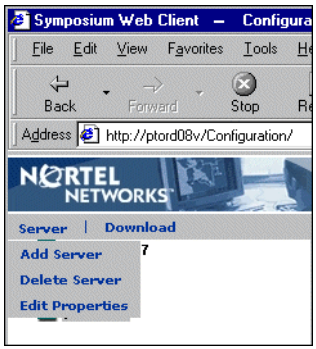
Introduction

Once you have logged on to Symposium Web Client as the user *webadmin*, you can add servers in Symposium Call Center Server in the Configuration component by accessing the Server menu from the toolbar.

Notes:

- The Server menu is visible only when you log on to Symposium Web Client as the user *webadmin*.
- Before you can add a newly configured server in Symposium Call Center Server, you must first change the server's default password. Since Symposium Web Client does not allow you to change this password in the Configuration component, you must use the Symposium Call Center Server client to log on to brand new servers for the first time. Once you change the default password, you can then use Symposium Web Client to add the desired servers according to the following procedure.

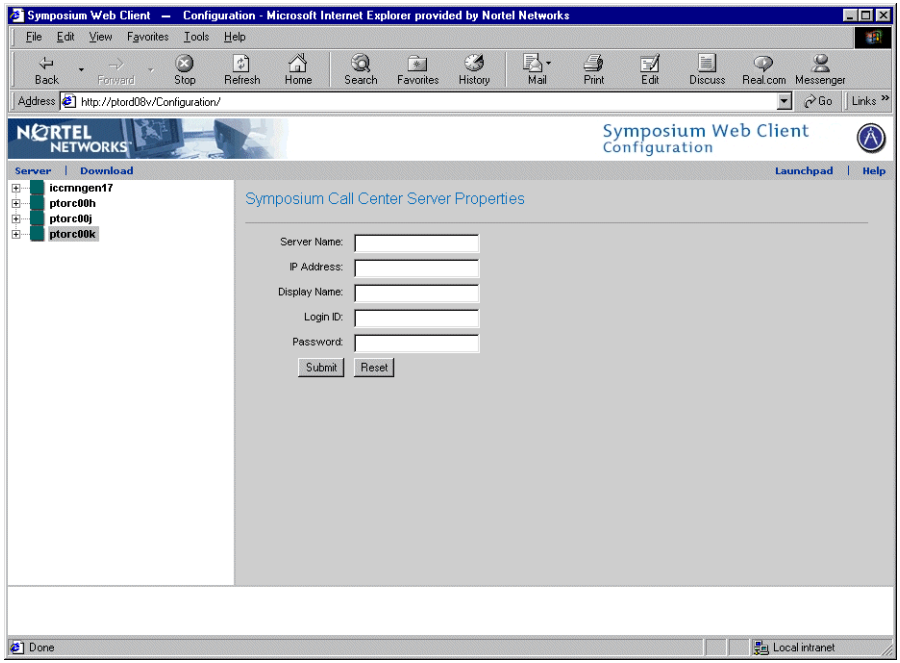
Configuration → Server menu



Note: From the Server menu, you can also delete existing servers in Symposium Call Center Server, or edit the properties of an existing server that has already been added to Symposium Web Client.

After clicking Server → Add Server, the Symposium Call Center Server Properties window appears in the main pane.

Symposium Call Center Server Properties window



To add a server in Symposium Call Center Server

1 In the **Server Name** box, type the name of the server in Symposium Call Center Server.

2 Press **Tab**.

Result: The server's IP address automatically appears in the **IP Address** box.

Note: If you enter a server name without an IP address, that server name must be registered with the DNS server. When you tab out of the **Server Name** box, verify that the CLAN IP address appears in the IP Address box. If the word *Unknown* appears in this box, then the server name is not registered with either the DNS or the HOSTS table. In this case, you must enter the server's IP address in the **Server Name** box. For more

information on manually updating the HOSTS table, see “Did you configure a name resolution server?” on page 527.

3 In the **Display Name** box, type the name of the server in Symposium Call Center Server as you want it to appear on the system tree in Symposium Web Client.

Result: The system automatically assigns a display name that is the same as the server name. If you want to enter a different display name, it must be a unique name.

4 In the **Login ID** box, enter your Login ID for Symposium Call Center Server.

5 In the **Password** box, enter your password for Symposium Call Center Server.

6 Click **Submit**.

Result: The server is acquired and now appears on the server tree in the left pane of the window. Click the plus symbol (+) beside the server name to access the server.

ATTENTION

The Symposium Call Center Server Login ID and Password that you specify when configuring a new server in Symposium Web Client must match an existing logon ID and password that an administrator has configured on Symposium Call Center Server. Therefore, if an administrator uses the Symposium Call Center Server client to change a server Login ID that you have *already* entered in Symposium Web Client, then you must update the Login ID box in the Configuration component of Symposium Web Client to match the new Login ID. Likewise, if an administrator changes the Symposium Call Center Server password using the Symposium Call Center Server client, then you must update the password in the Configuration component of Symposium Web Client to match the new password.

Note: If you need to change the CLAN IP address of the server in Symposium Call Center Server after you have added it in Symposium Web Client, then you must perform a series of steps to ensure that you do not lose customized data, such as historical reports and real-time displays. For

more information, see “To change the IP address of a server in Symposium Call Center Server” on page 389.

To change the IP address of a server in Symposium Call Center Server

To successfully change the CLAN IP address of a server in Symposium Call Center Server without losing customized data, such as user-created historical reports, real-time displays, and user assignments, you must perform the following procedures:

1. On the server in Symposium Call Center Server, change the server’s IP address. For more information, see the Configuration (Nbconfig) section in the *Symposium Call Center Server Installation and Maintenance Guide* for Release 4.2.
2. On the Symposium Web Client application server, use the DOS prompt to ping the server in Symposium Call Center Server and ensure that the new IP address is valid.
3. On the application server, or any client computer that accesses Symposium Web Client, open the Symposium Call Center Server Properties window in the Configuration component of Symposium Web Client and change the IP address of the server to match the address that you typed in step 1.
4. On each application server in your network that connects to this server in Symposium Call Center Server, run the Change IP Address Utility to register the changed IP address. For more information on this utility, see “To use the Change IP Address Utility” below.

To use the Change IP Address Utility

After you have performed the first three procedures listed above, you must run the Change IP Address Utility on each application server in your network that accesses the server in Symposium Call Center Server whose IP address you have changed. This utility ensures that customized data, such as user-created historical reports and user assignments, is not lost when you change the IP address.

1 On the application server, navigate to the following file:

c:\Program Files\Nortel Networks\WClient\Apps\SupportUtil\changeip.exe

where c: is the drive on which you have installed Symposium Web Client.

2 Double-click the changeip.exe file.

Result: The Change IP Address Utility opens.

3 In the Type the old IP address box, type the server's old IP address.

4 In the Type the new IP address box, type the new server's new IP address.

5 Click **OK**.

Result: The utility confirms that the old IP address matches the address stored in the database and that the new IP address you typed is valid. It then updates the local access file with the new information. The utility notifies you if it encounters an error, in which case, you can consult the log file for details. The log file is located in the same folder as the utility and is called ip2ip.log.

Configuring resources

Introduction

You can configure resources using two different methods:

- uploading bulk data using the Symposium Configuration spreadsheets
  or
- individually, using the web-based user interface

Note: You cannot acquire resources such as CDNs, routes, voice ports, IVR ACD-DNs, and phonesets through the Symposium Configuration spreadsheets. You must use the web-based interface in Configuration for resource acquisition.

Using spreadsheets to upload data to Symposium Call Center Server

By using the Symposium Configuration spreadsheets, you can save yourself time when configuring a new call center. Instead of entering the data for each resource individually, you can upload all of the configuration data that you have entered in the spreadsheet simultaneously. When you upload the data from the spreadsheet, you can choose to upload all of the configuration items at once, or only a portion of them.

Notes:

- You must be logged on to Symposium Web Client as the default administrator, *webadmin*, to upload and download data, and to download the spreadsheet template from the Configuration component.
- If you are logged on as *webadmin*, but still cannot download the spreadsheet templates from the application server, it may be because IIS Lockdown and URLScan are enabled on the application server. You must either download the spreadsheets before enabling these security features, or temporarily relax the URLScan feature by modifying the urlscan.ini file to enable the downloading of files that end with .exe (such as the Configuration spreadsheets). For more information, see “To temporarily edit the urlscan.ini file” on page 224.

Based on your call center server (M1/CSE 1000, DMS/MSL-100, or NCC), you can upload the following configuration data using the corresponding Symposium Configuration spreadsheet:

■ Users	■ Skillsets
■ DNISs	■ Global Settings
■ Phonesets and Voice Ports	■ Call presentation classes
■ Routes	■ IVR ACD DNs
■ CDNS	■ Threshold Classes* *Agent, Skillset, Application, IVR ACD-DN, Route, Nodal
■ Activity Codes	■ Network Parameters

Notes:

- The number of agent to skillset and agent to supervisor assignments that you can upload from the Symposium Configuration spreadsheets is restricted due to the Microsoft Excel limit of 256 columns per worksheet.
- Although you can upload supervisor and agent configuration data using the Configuration spreadsheets, you must modify and delete this data using the Contact Center Management component, not the Configuration component.
- Once you upload a phoneset or voice port, you cannot modify it. A phoneset or voice port that has been uploaded can be deleted and a new phoneset or voice port added. For example, once you have uploaded a voice port, you cannot change it to a phoneset (and vice versa). Instead, you must delete the voice port and add a new phoneset (or vice versa).

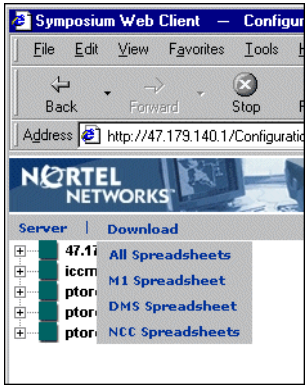
Downloading the Symposium Configuration spreadsheet template

Before you begin, you must download the appropriate Symposium Configuration spreadsheet templates from the Configuration component by accessing the Download menu on the toolbar.

Notes:

- The Download menu is visible only when you log on to Symposium Web Client as the user *webadmin*.
- If you are logged on as *webadmin*, but still cannot download the spreadsheet templates from the application server, it may be because IIS Lockdown and URLScan are enabled on the application server. You must either download the spreadsheets before enabling these security features, or temporarily relax the URLScan feature by modifying the urlscan.ini file to enable the downloading of files that end with .exe (such as the Configuration spreadsheets). For more information, see “To temporarily edit the urlscan.ini file” on page 224.
- The number of agent to skillset and agent to supervisor assignments that you can download to the Symposium Configuration spreadsheets is restricted due to the Microsoft Excel limit of 256 columns per worksheet.

Configuration → Download menu



When you download a spreadsheet, four files are included: the spreadsheet file (.xls), the validation file (.xml), the Help file (.chm), and the Asian validation file (.xml). Make sure all of these files reside in the same folder on your computer after downloading.

For step-by-step procedures about downloading the Symposium Configuration spreadsheet templates, see the Symposium Web Client online Help. From the Symposium Web Client toolbar, click Help → Contents, and from the Contents tab, click Configuration → Procedures → Spreadsheet procedures for detailed information.

Using the Symposium Configuration spreadsheet template

Once you download the appropriate Symposium Configuration spreadsheet template for your call center (that is, M1/CSE 1000, NCC, or DMS/MSL-100), you can enter configuration data directly into the spreadsheet, or you can copy configuration data into the spreadsheet from various sources:

- existing spreadsheets
- M1 Data Extraction Tool spreadsheets
- personnel files (for user names)

ATTENTION

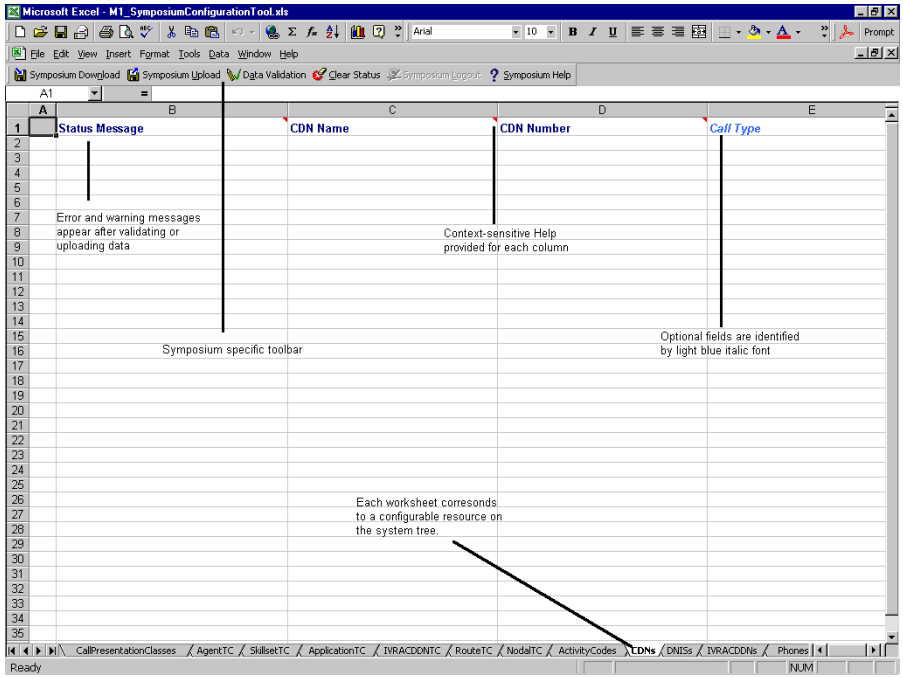
You must *copy* data from any existing spreadsheets into the Symposium Configuration spreadsheet templates. You cannot upload data directly from an existing spreadsheet. For more information, see the *Symposium Call Center Server Data Extraction Tool User's Guide for the Meridian 1*.

The Symposium Configuration spreadsheet has its own toolbar that allows you to perform the following tasks:

- Download existing configuration data from Symposium Call Center Server.
- Upload configuration data to Symposium Call Center Server.
- Validate the data that you have entered into the spreadsheet.
- Clear error messages from the spreadsheet after you have validated and repaired the data.
- Log off the application server.
- Access Symposium Help.

Configuration spreadsheet

When opening the Symposium Configuration spreadsheets, a Microsoft Excel message asks if you want to enable all macros. Click **Yes** to enable all macros.



Viewing the version of the Symposium Configuration spreadsheet

For information purposes only, you can view the version number of the spreadsheets that you download from the application server. The version number changes if the spreadsheet has been updated with new functionality and placed in a new Symposium Web Client build. To view the version number, click File → Properties. The version number appears in the **Author** box on the **Summary** tab.

ATTENTION

You must not change the version number shown on this tab. If you change the version number, then the Symposium Configuration spreadsheet will not function correctly.

Language support in the Symposium Configuration spreadsheets

You can type data in one of five languages in the Symposium Configuration spreadsheets (English, French, German, Japanese, and Chinese) and ensure that it is validated correctly by choosing the appropriate language in the Data Upload window and confirming that the correct validation file is located in the same folder as the spreadsheet. The following table outlines which validation file is used with each type of data.

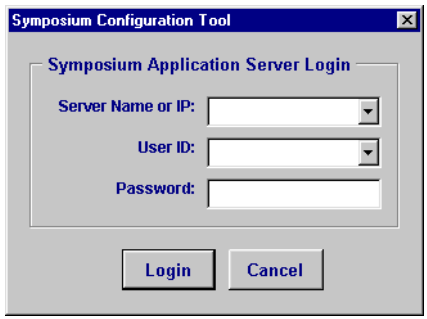
Note: You must ensure that the correct validation file is located in the same folder as the spreadsheet before you validate or upload data to the server.

Server type	Language in which data is written	Validation file
M1	English, French, or German	M1_Validation.xml
	Japanese or Chinese	M1_Validation_Asian.xml
DMS	English, French, or German	DMS_Validation.xml
	Japanese or Chinese	DMS_Validation_Asian.xml
NCC	English, French, or German	NCC_Validation.xml
	Japanese or Chinese	NCC_Validation_Asian.xml

Uploading data to Symposium Call Center Server

Once you have entered the configuration information into the spreadsheet, validate your data by clicking **Data Validation** on the toolbar. After you have corrected any invalid information and have successfully validated the information, click **Symposium Upload** on the toolbar.

The system prompts you to log on to the application server by entering the application server IP address before uploading data.



Data Upload - Symposium Configuration Tool window

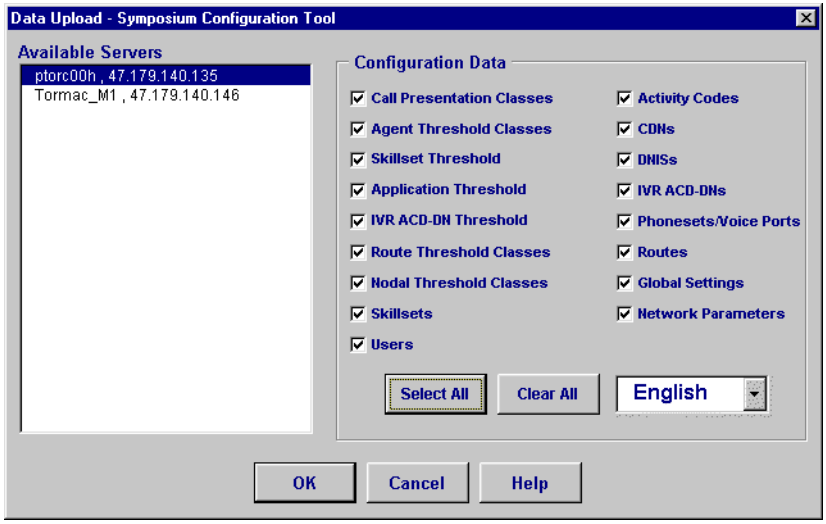
In the resulting Data Upload - Symposium Configuration Tool window, you must select the server in Symposium Call Center Server to which you want to upload the data (or select the appropriate NCC server if you are working in the NCC spreadsheet). In the **Configuration Data** section, indicate the type of data you want to upload.

Finally, from the drop-down list of languages, select the language in which the data you are uploading is written. You can choose from English, French, German, Japanese, and Chinese.

ATTENTION

To ensure that the system properly validates the data you are uploading, the appropriate validation file must be located in the same folder as the spreadsheet. For a list of the validation files, see “Language support in the Symposium Configuration spreadsheets” on page 396.

Note: The **Available Servers** box displays the servers that correspond to the Configuration spreadsheet you are using. For example, if you are using the M1_SymposiumConfigurationTool.xls spreadsheet, NCC servers do not appear in the **Available Servers** box during uploading. To upload data to an NCC server, you must use the NCC_SymposiumConfigurationTool.xls spreadsheet.



As your data uploads, the Current Status box displays the records that are being read. After the upload process is complete, the Summary Status box lists the data that was successfully uploaded, as well as any errors that occurred. If there are any errors, they also appear in the **Status Message** column of the spreadsheet.

You cannot acquire resources such as CDNs, routes, voice ports, IVR ACD-DNs, and phonesets through the Symposium Configuration spreadsheet. You must use the web-based interface in Configuration for resource acquisition.

Note: For step-by-step procedures about the Symposium Configuration spreadsheets, see the Symposium Web Client online Help. From the Symposium Web Client toolbar, click Help → Contents, and from the Contents tab, click Configuration → Procedures → Spreadsheet procedures.

Downloading data from Symposium Call Center Server

You can download configuration data from Symposium Call Center Server to the Symposium Configuration spreadsheets. You can do this to review your configuration data, or to make changes to the data and then upload it back to the server in Symposium Call Center Server.

Before you download data from Symposium Call Center Server, you must download the appropriate Symposium Configuration spreadsheet from the Configuration component. To make sure you do not overwrite an existing Symposium Configuration spreadsheet, rename the spreadsheet or save it in a different directory when downloading.

Once you download the new Symposium Configuration spreadsheet, open the spreadsheet and click **Symposium download** on the toolbar. Provide the appropriate information for the Symposium Call Center Server from which you are downloading data and for the application server.

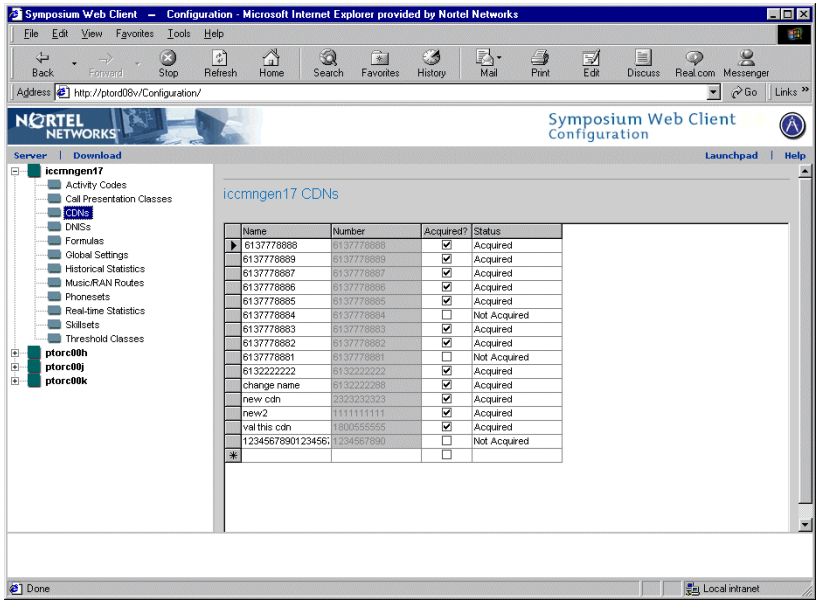
Note: For step-by-step procedures about the Symposium Configuration spreadsheets, see the Symposium Web Client online Help. From the Symposium Web Client toolbar, click Help → Contents, and from the Contents tab, click Configuration → Procedures → Spreadsheet procedures.

Using the Configuration user interface

You can add configuration resource data using the Configuration user interface. When you click the resource on the system tree, the corresponding data table appears on the right side of the window. Click an empty row and type the configuration data in the appropriate columns. When you exit a row, the information is automatically saved in Symposium Call Center Server.

Note: New configuration data is saved to Symposium Call Center Server when you leave the row in which you have entered the data. Do not click **Back** or **Refresh** on the Internet Explorer button bar to save or refresh the data in the table. To refresh the table while working with Routes, CDNs, Phonesets, and IVR ACD-DNs, click the **Refresh** button in the Configuration window; to refresh the data while working with any other type of data, you must click the server name on the system tree.

Configuration user interface



You can edit information in individual cells by clicking directly on the cell and modifying the data. You can delete entire rows by selecting the row and pressing **Delete** on your keyboard. To save data, use your mouse to click a different row, or press **Tab** to move to the next row.

What's next?

Create the Symposium Call Center Server users, designate them as supervisors, agents, or supervisor/agents, and assign agents to supervisors.

Section C: Contact Center Management

In this section

Overview	402
Working in supervisor view	404
Working in agent view	408
Working in skillset view	414
Working in assignments view	417
Adding Symposium Call Center Server users	420
Using the XML automated assignments feature	426

Overview

Introduction

Once you add and configure each server in Symposium Call Center Server, you can use the Contact Center Management component to perform the following tasks:

- Add, edit, view, or delete users on a server in Symposium Call Center Server.
- Add, edit, view, or delete agent to supervisor assignments.
- Add, edit, view, or delete agent to skillset assignments.
- You can also use Contact Center Management to quickly assign agents to existing partitions, instead of opening the Access and Partition Management component to do so.

This section provides a high-level overview on adding Symposium Call Center Server users, designating them as supervisors, agents, or supervisor/agents, editing their profiles, and assigning agents to supervisors and skillsets.

This section assumes that, as an administrator, you

- have the appropriate access class to perform all functions in Contact Center Management (the *Add/Edit/Delete Agents and Supervisors* access level under the CCM access heading, and the *Schedule Assignments* access level under both the Agent to Supervisor Assignment and Skillset Assignment access headings)
- have no partitions or supervisor/reporting agent combinations assigned to you and can, therefore, view all data in Contact Center Management

For detailed information about working in Contact Center Management, refer to the *Symposium Call Center Web Client Supervisor's Reference Guide*, or refer to the step-by-step procedures in the online Help.

Main data views

Contact Center Management can be separated into the following four main data views, each accessible from the View/Edit menu:

- Supervisors (this is the default view that appears when you first open Contact Center Management)
- Agents
- Skillsets
- Assignments

To switch from one type of data, or view, to the next, click the desired option from the View/Edit menu.

When you click any of these options, the system loads the corresponding type of data in the system tree. Before you can work with each type of data, you must first click a server name in the tree to log on to the server and view its agents, supervisors, and skillsets. If you work in a networked environment, the system tree contains multiple servers, with each server representing a call center in the network.

For more information on each of these data categories, see the corresponding section below.

Notes:

- To create new users, click the desired option from the Add menu. You can choose from Agent, Supervisor, or Supervisor/Agent. When you click one of these options, the corresponding new user details window appears, where you can type the user's properties. For more information on creating users, see the online Help.
- To create new agents, in addition to the above option, you can also right-click a supervisor in the system tree, and then select Add Agent from the resulting pop-up menu.
- When you click **Refresh,** the system collapses the tree, closes the window in which you are currently working, and reloads the supervisor view. Once reloaded, you must click to log on to a server again.

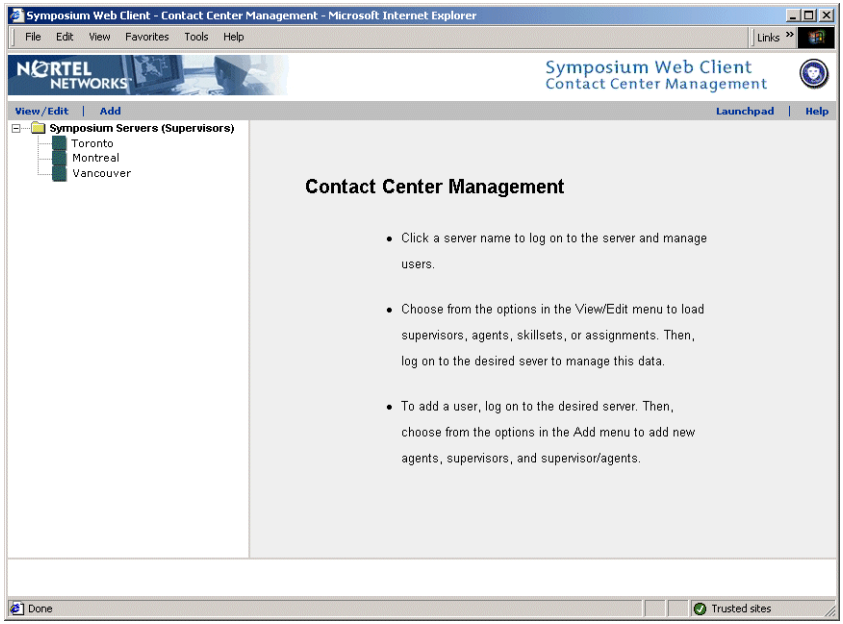
Working in supervisor view

Introduction

When you open Contact Center Management from the Symposium Web Client launchpad, it opens in supervisor view. This view enables you to quickly see the supervisors who are configured on each server on the system tree and list the agents assigned to each supervisor. You can use this view to immediately assign agents to supervisors (ad hoc assignments).

Notes:

- To create saved and scheduled assignments, you must use the assignments view. For more information, see “Working in assignments view” on page 417.
- To add new supervisors, use the Add menu.

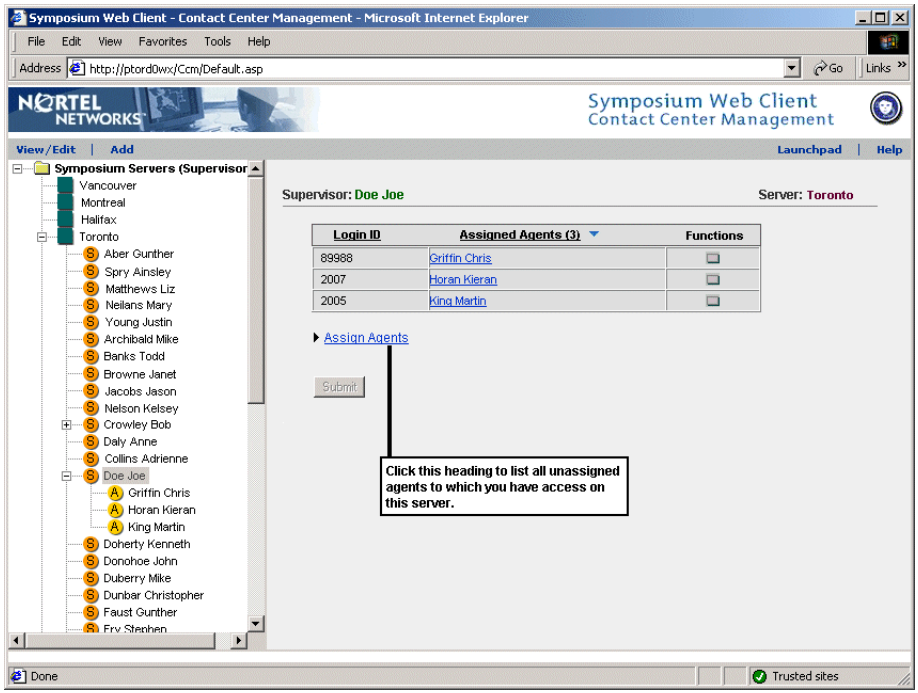


Ad hoc agent to supervisor assignments

To work with agents and supervisors, users must first log on to the appropriate server in the system tree. The server expands to reveal all the supervisors configured on it. Click a supervisor in the tree to open the Supervisor window and see the supervisor's reporting agents and their corresponding logon IDs.

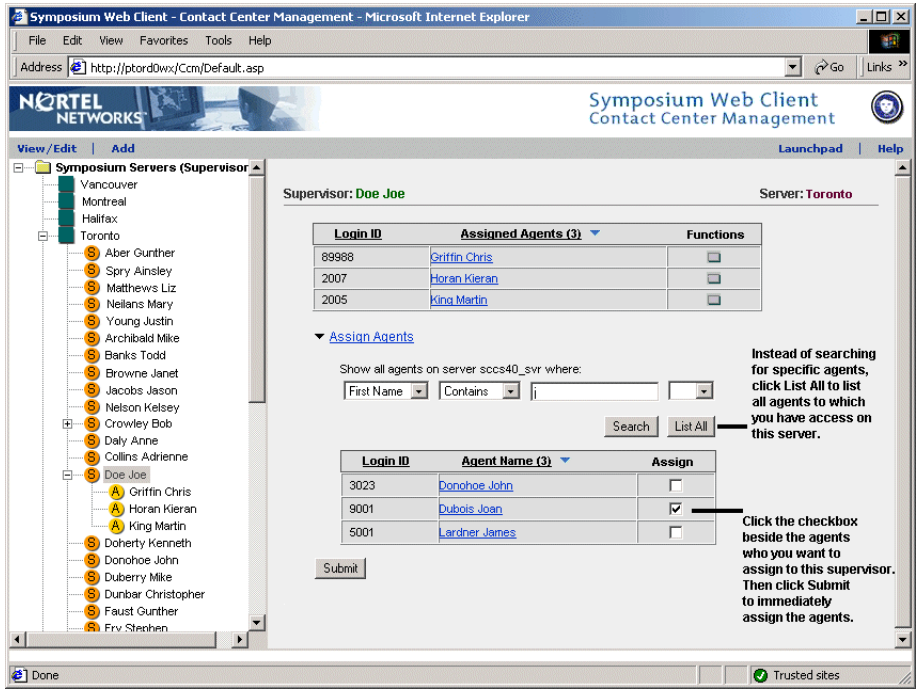
Users with administrator rights (that is, users who have been granted basic access to all Symposium Web Client components and who have no partitions or supervisor/reporting agents assigned to them) automatically see all supervisors and agents in all windows of Contact Center Management. However, users who have been assigned a partition containing agents, or a partition and a supervisor/reporting agent combination, see only those agents to whom they have been given access. For more information, see "Partitions and supervisor/reporting agent combinations in Contact Center Management" on page 473.

Note: To create saved and scheduled assignments, you must use the assignments view. For more information, see "Working in assignments view" on page 417.



To quickly assign new agents to a supervisor, click **Assign Agents**. The agent search feature appears, enabling you to search for *specific* agents by up to five criteria (first name, last name, login ID, department, or comment), or to list *all* agents configured on the server (only those agents included in the partitions and supervisor/reporting agent combinations assigned to you). When you click **Search**, or **List All**, the agents appear in a new table.

Note: Partitions and supervisor/reporting agent assignments control the agent data that users can see in Contact Center Management. To give a user access to all agents, do not assign a partition to the user. To give a user access only to their reporting agents, assign the user a partition (even if it contains no agents) and the supervisor/reporting agent combination containing the user's agents. For more information on partitions and supervisor/reporting agent combinations in Contact Center Management, see "Partitions and supervisor/reporting agent combinations in Contact Center Management" on page 473.



When you have found the agents you want to assign to the supervisor, click the **Assign** check box beside their names, and then click **Submit**. The system immediately assigns the agents to the supervisor.

Note: Each agent can be assigned to only one supervisor at a time. Therefore, when you assign an agent to a supervisor, you unassign the agent from his or her current supervisor.

Tip: You can also assign agents to the supervisor, one agent at a time, using the drag and drop feature. On the system tree in supervisor view, locate the agent who you want to assign to the supervisor. Left-click the agent icon and, while still holding down the left mouse button, drag the icon over the desired supervisor icon. Release the mouse button to immediately assign the agent to the supervisor.

Working in agent view

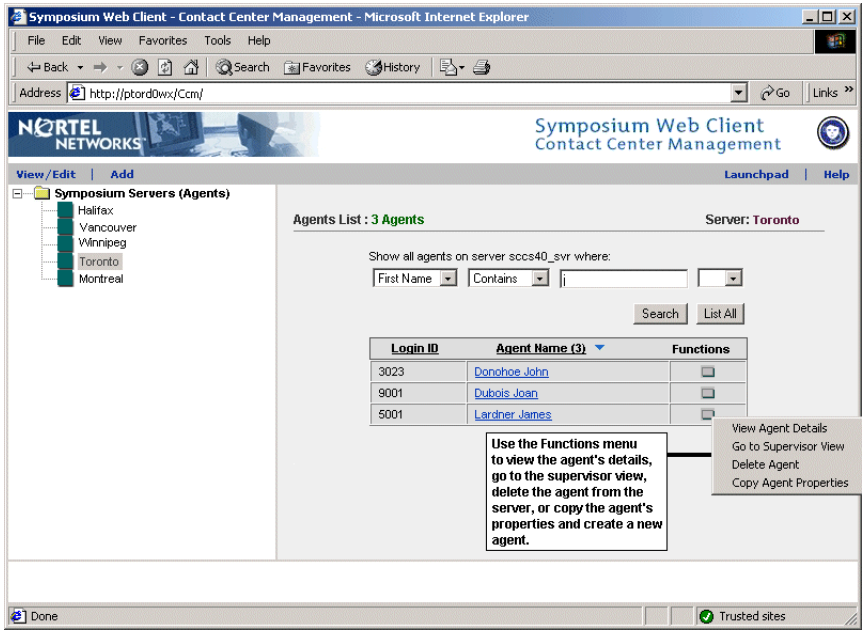
Introduction

Note: In the following section, the term “agent” also includes users who are supervisor/agents, as the agent view enables you to work with both types of users.

The agent view enables you to search for particular agents or list all agents on a server. Once you have located the desired agent, you can

- view and edit the agent’s properties, including the skillsets and partitions to which the agent is assigned
- delete the agent from the server
- quickly create a new agent by copying the current agent’s properties

To open the agent view, click View/Edit → Agents. Then, click the desired server in the system tree to log on to the server and work with the agents configured on it. When you click a server in the system tree, the Agents List window appears. In this window, you can use the agent search boxes to locate specific agents, or click **List All** to list all agents on the selected server.

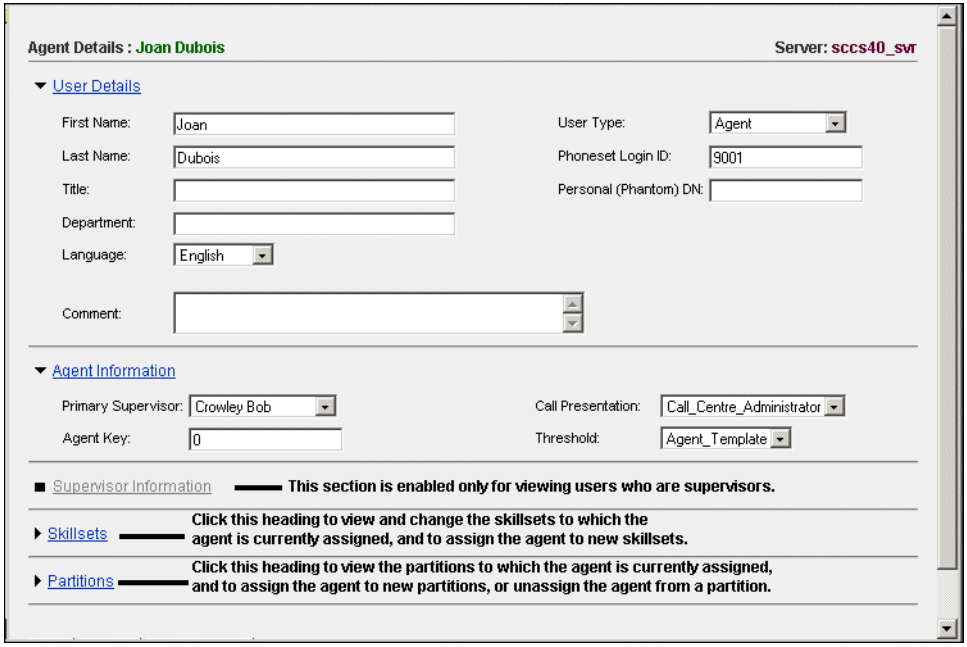


Viewing or editing the agent details

In the Agents List window, from the table of agents who you have located through your search, there are two ways in which you can view or edit an agent's details:

- Click the desired agent's name.
- Click **Functions** beside the desired agent, and then select **View Agent Details** from the resulting pop-up menu.

When you click either of these options, the Agent Details window appears, enabling you to view all of the agent's properties, such as name, login ID, supervisor information, and the skillsets and partitions to which the agent is assigned.



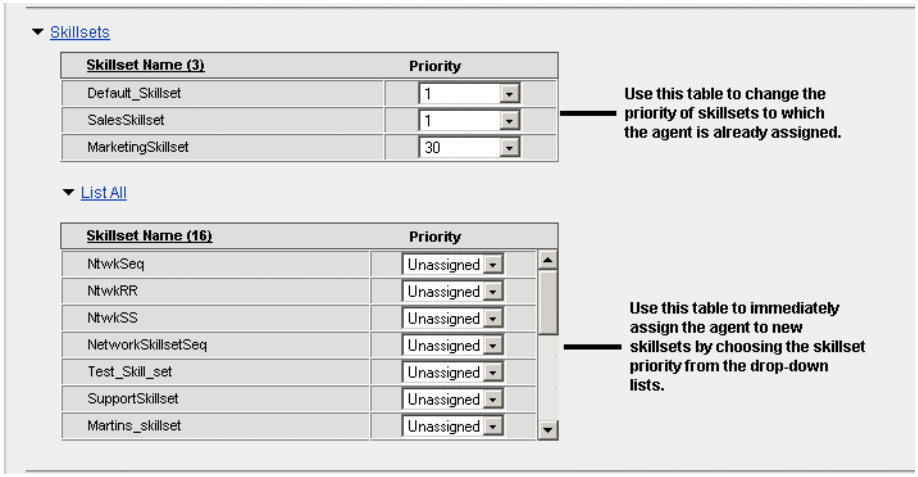
Use the User Details and Agent Information sections of this window to view and change information about the agent, such as the name, login ID, user type, and primary supervisor.

In addition, when you create supervisors and supervisor/agents, the Supervisor Information section is enabled and allows you to assign these users a Web Client user ID and password.

This information is required if the user is going to log on to the application server and use Symposium Web Client. When you are finished adding the user's details, you must click **Submit** to save your changes.

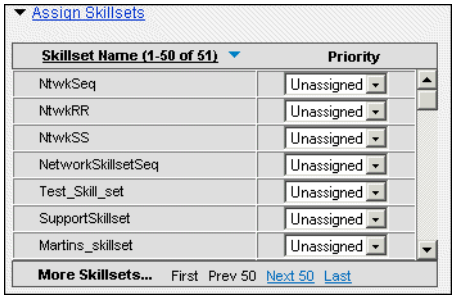
Viewing or editing ad hoc agent to skillset assignments

Click the **Skillsets** heading in the Agent Details window to view the skillsets to which the agent is assigned and change the skillset priority. Click **List All** to list all configured skillsets on the server and assign the agent to new skillsets.



Windows 98 and ad hoc agent to skillset assignments

If you have the Windows 98 operating system, and the number of skillsets that you can choose from to assign to an agent is greater than 50, then the **List All** section of this window changes slightly, as shown in the following graphic:



In this case, the skillsets that you can choose from are listed in the table, 50 skillsets at a time. To view all skillsets (in groups of 50 or less), use the **Prev 50**, **Next 50**, or **Last** links at the bottom of the table.

Viewing or editing partition assignments

Click the **Partitions** heading in the Agent Details window to view the partitions to which the agent is assigned and assign the agent to new partitions.

Click the check box beside the partition name to assign the agent to the partition. When you click **Submit**, the agent is automatically included in the partition you indicated (and can, therefore, be viewed by the supervisors to whom this partition is assigned).

Deselect the check box beside the partition name to unassign the agent from the partition.

Note: Before you unassign an agent from a partition, ensure that the agent's supervisor can still see the agent in Contact Center Management, Historical and Real-Time Reporting, either because the agent is included in another partition assigned to the supervisor, or the supervisor is assigned a supervisor/reporting agent combination (which automatically includes the agent).

Deleting agents in agent view

On the Functions menu in agent view, click **Delete Agent** to delete the agent from the server.

Note: You can also right-click the agent in the system tree, and then select **Delete Agent** from the resulting pop-up menu.

Copying an agent's properties

You can also use the Functions menu in the Agents List window to quickly create a new agent by copying the properties of an existing agent.

When you click **Copy Agent Properties** on the Functions menu, the system copies the following properties from the existing agent into the New Agent Details window:

- skillset assignment
- department
- user type
- language
- comment
- supervisor
- call presentation

- threshold
- agent key

To create the new agent, you must type in the new agent's name and phoneset logon ID, you may also change any of the copied properties, and then press **Submit** to save your changes. The system saves the agent under the supervisor that you specified, and the agent's icon appears in the system tree.

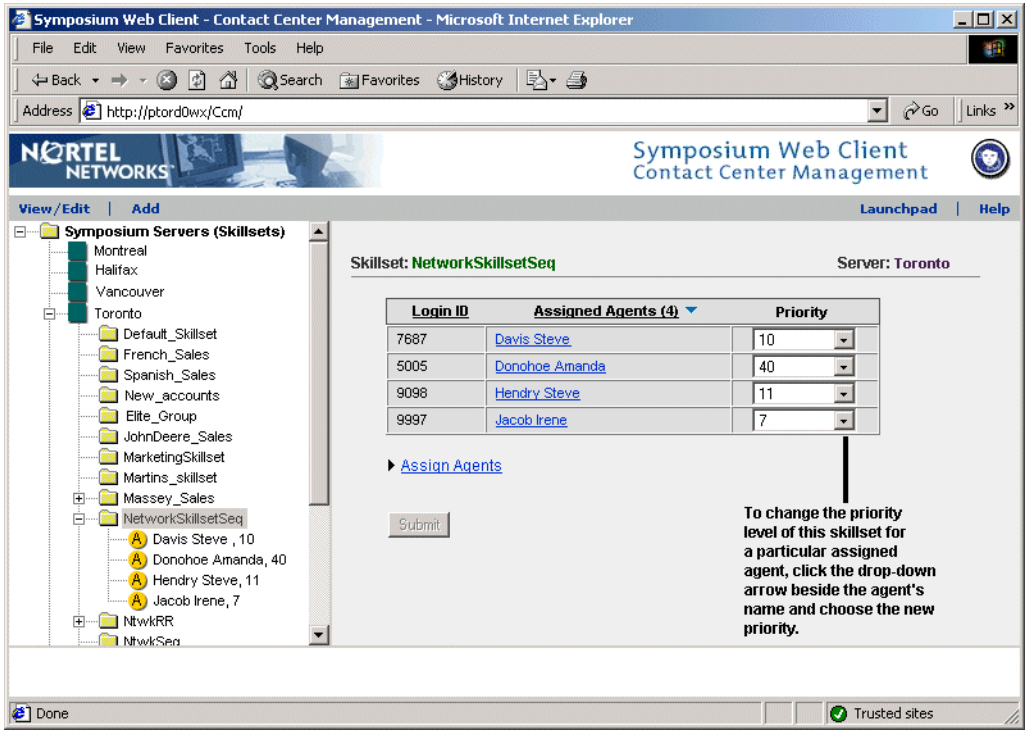
Working in skillset view

Introduction

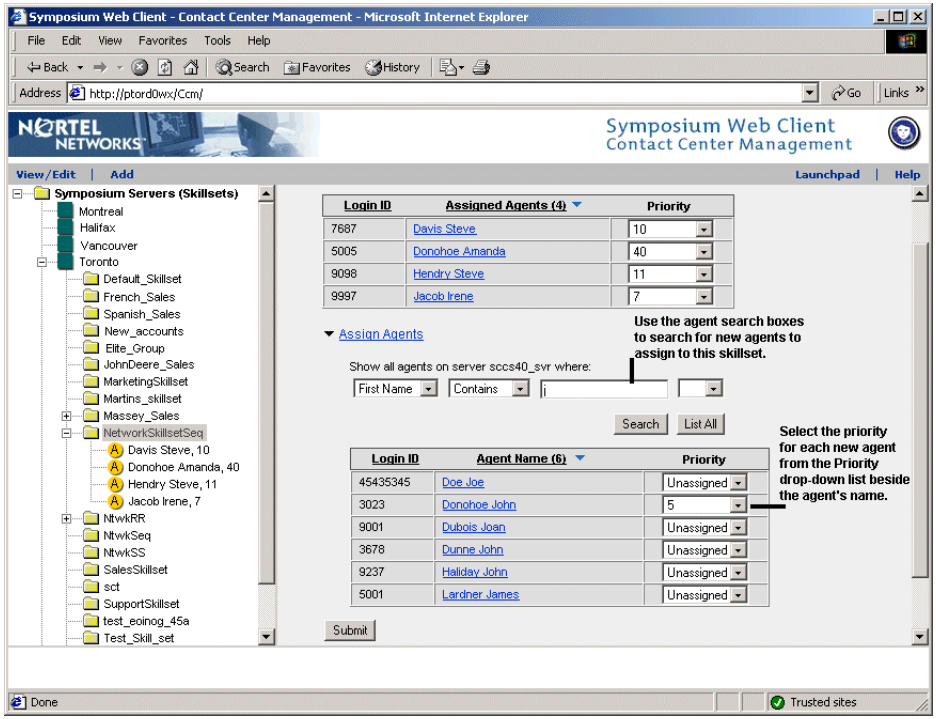
The skillset view enables you to create new ad hoc agent to skillset assignments and change the priority of skillsets already assigned to agents. Click View/Edit → Skillsets to change the system tree to skillset view. Then click the desired server in the system tree to log on to the server and work with the skillsets and agents configured on it. When you click a skillset in the system tree, the Skillset window appears, listing the agents who are currently assigned and their priority for this skillset.

Ad hoc agent to skillset assignments

In the Skillset window, you can immediately assign an agent to a new skillset or change the priority of an assigned skillset. To change the priority of an agent already assigned to the skillset, from the **Priority** drop-down list, choose the new priority. Then click **Submit** to save your changes.



To immediately assign a *new* agent to the skillset, click the **Assign Agents** heading. Just as in supervisor view, when you click this heading, the agent search feature appears, enabling you to search for *specific* agents by up to five criteria (first name, last name, login ID, department, or comment), or to list *all* agents configured on the server (only those agents included in the partitions and supervisor/reporting agent combinations assigned to you). When you click **Search**, or **List All**, the agents appear in a new table.



From the list of unassigned agents, choose the skillset priority for each agent. Then click **Submit** to save your changes. The system immediately assigns the agents to the skillset with the priority you chose.

Note: To create saved or scheduled assignments, you must use the assignments view. For more information, see “Working in assignments view” on page 417.

Working in assignments view

Introduction

The assignments view enables you to view and edit saved and scheduled agent to skillset and agent to supervisor assignments and create new saved and scheduled assignments. Click View/Edit → Assignments to load the assignment data in the system tree. Then click the desired server in the system tree to log on to the server and work with the assignments configured on it.

Note: To create ad hoc (unscheduled) agent to skillset assignments, use the skillset view. To create ad hoc agent to supervisor assignments, use the supervisor view.

ATTENTION

Symposium Web Client only recognizes assignments that you schedule in Contact Center Management; likewise, the Symposium Call Center Server client only recognizes assignments that you schedule through its scheduling component. Therefore, when scheduling assignments, you must use either the Contact Center Management portion of Symposium Web Client *or* the Symposium Call Center Server client exclusively. You cannot use a combination of both client components to schedule assignments.

This section gives a brief overview of the assignments view. For more information on this view, including assignment scenarios, and an example of scheduling an assignment and creating a reset assignment, see the *Symposium Call Center Web Client Supervisor's Reference Guide*.

Assignment types

There are two types of assignments that you can create in Contact Center Management:

- **Agent to supervisor assignments** You can create agent to supervisor assignments to automatically change supervisor assignments for multiple

agents. You can use agent to supervisor assignments to reassign agents when supervisors go on break or vacation.

- **Agent to skillset assignments** You can create agent to skillset assignments to temporarily assign agents to different skillsets for shifts when fewer agents are available, to cover other agents' breaks, or when agents are sick, on vacation, or on a course.

An agent to skillset assignment makes multiple agents active or inactive for multiple skillsets. When an assignment is run, it changes the skillset priority of each agent who has been added to the assignment. It can make an agent inactive for a skillset by changing the agent's priority to Standby, or it can make an agent active for a skillset by changing the agent's priority to a value from 1 to 48 (with 1 being the highest priority for the skillset).

In assignments view, you can save and schedule the assignments to take effect at a later date, and you can create reset assignments to revert the call center to the original configuration that existed before scheduled assignments are run. You create ad hoc assignments (those that are effective immediately) in the skillset or supervisor views. For more information, see "Ad hoc agent to supervisor assignments" on page 405, or "Ad hoc agent to skillset assignments" on page 414.

Note: To create and run multiple assignments automatically, you can use the XML automated assignments feature. For more information, see "Using the XML automated assignments feature" on page 426.

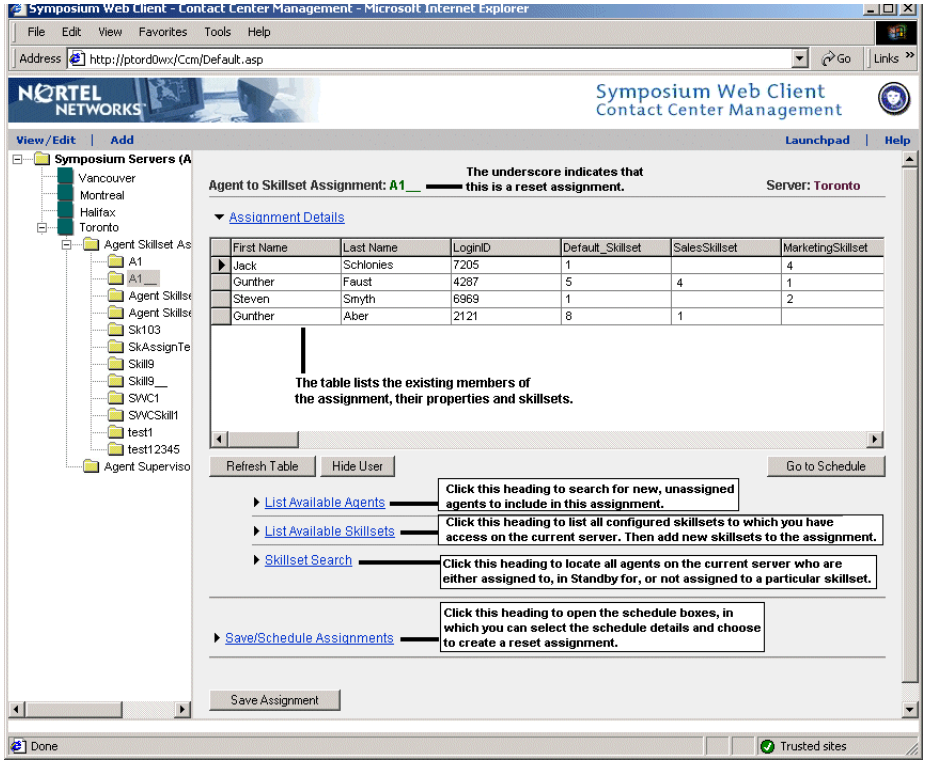
Working with scheduled assignments

In assignments view, you can either

- work with *existing* scheduled assignments by clicking the assignment name in the system tree
- add *new* agent to skillset or agent to supervisor assignments by right-clicking the **Agent Skillset Assignments** or **Agent Supervisor Assignments** folder, and then choosing **Add Assignment** from the resulting pop-up menu

When you log on to a server in the system tree, it expands to reveal the Agent Skillset Assignments and Agent Supervisor Assignments folders. Double-click the appropriate folder to view the list of assignments. Then click the assignment name to open the assignment window and view the assignment details in a table. Based on the type of assignment that you click in the system tree, either the Agent to Skillset Assignment window or the Agent to Supervisor Assignment window appears.

The following graphic shows the assignment details that appear when you click an existing agent to skillset assignment from the system tree.



For details on working in this window, see the *Symposium Call Center Web Client Supervisor's Reference Guide*.

Adding Symposium Call Center Server users

Introduction

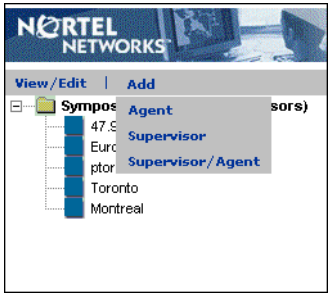
The users you add in Contact Center Management are Symposium Call Center Server users—the agents, supervisor/agents, and supervisors who work in the call center. Agents do not need to log on to the application server to use Symposium Web Client and, therefore, do not have a Web Client user ID and password.

However, when you are creating Symposium Call Center Server users in Contact Center Management, you can give the supervisors and supervisor/agents who need to use Symposium Web Client a Web Client user ID and password. When you do so, the user's profile is automatically copied to the Access and Partition Management component, where you must finish configuring the user's Web Client profile by assigning basic access rights, access classes, partitions, report groups, and supervisor/reporting agent combinations. For more information on creating Web Client users, see "Adding and configuring users" on page 462.

To add users in Contact Center Management, you must first log on to a server in the system tree in any of the four data views (supervisor, agent, skillset, or assignment). Then, when you are logged on to the server on which you want to create the user, select the appropriate option from the Add menu. You can choose from one of the following options:

- Agent
- Supervisor
- Supervisor/Agent

Contact Center Management → Add menu



When you select an option from this menu, the corresponding new user details window appears, with sections for entering the new user's properties. For example, if you are adding a new supervisor, the New Supervisor Details window appears.

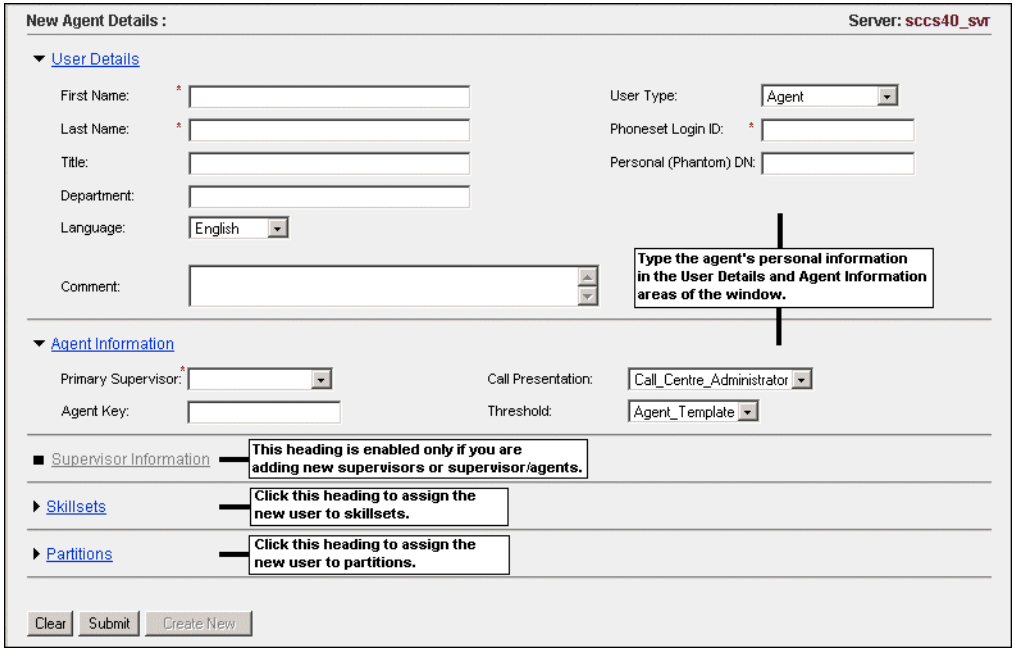
Notes:

- To add agents only, instead of using the Add menu, you can use a pop-up menu on the system tree in supervisor view. Right-click the supervisor under whom you want to create the new agent, and, from the resulting pop-up menu, click **Add Agent**. The New Agent Details window appears, with the supervisor information already filled in. You can change this information, or leave it as is. When you are finished adding the agent details, click **Submit** to save your changes. For more information on each section of the user details window, see below.
- If you need to delete users, you must do so in Contact Center Management; you cannot delete users through the Configuration component's user interface or spreadsheets.

To add agents

The following section outlines how to add new agents in Contact Center Management. For details on adding other types of users, see the online Help. When you log on to a server in the system tree and click Add → Agent, the new Agent Details window appears.

New Agent Details window

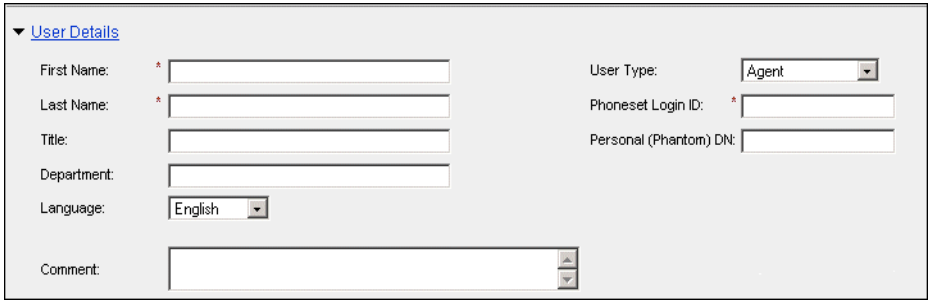


Entering user data

For entering user data, there is a **User Details** section, which is applicable to all user types, an **Agent Information** section, and a **Supervisor Information** section. The system allows you to enter information in these latter areas based on the type of user you selected from the Add menu.

Note: The mandatory fields in which you have to type or select information are indicated on the window by an asterisk (*) and include the first name, last name, phoneset login ID, and primary supervisor. The other mandatory fields (user type, call presentation, and threshold) do not have an asterisk beside them because they have default values. Select the appropriate values for the user you are adding.

User Details section



1. In the User Details section, you must type or select the following mandatory information about the agent:

   - first name
   - last name
   - user type
   - phoneset login ID

   All other fields are optional.

Agent Information section

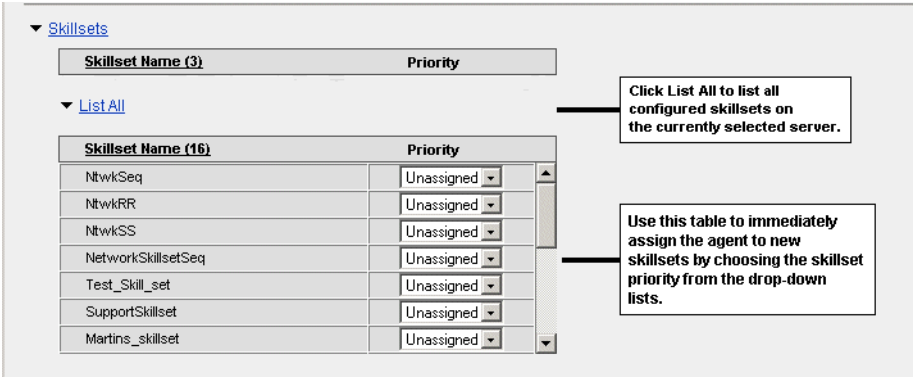
2. In the Agent Information section, you must type or select the following mandatory information about the agent:

   - primary supervisor
   - call presentation
   - threshold

   The agent key is optional.

3. After you have added the agent's personal information, click the **Skillsets** heading to assign the agent to skillsets and select the skillset priority.

Skillsets section



4. Click **List All** to open a table containing all the skillsets on the current server.

5. In the table, choose the priority numbers beside the skillsets to which you want to assign the new agent. You can also choose **Standby**.

Note: If your operating system is Windows 98 and the number of skillsets that you can choose from to assign to an agent is greater than 50, then the **List All** section of this window changes slightly. For details, see “Windows 98 and ad hoc agent to skillset assignments” on page 411.

6. To add the new agent to a partition, click the **Partitions** heading.

7. In the resulting table, click the check boxes beside the partitions to which you want to add the agent. Ensure that you add the agent to the partition assigned to the agent’s supervisor so the supervisor can see the agent in the real-time and historical reports, and in Contact Center Management.

8. Click **Submit** when you are finished entering the agent’s details. The agent is added in Symposium Call Center Server.

Supervisor information

When you add a supervisor or a supervisor/agent in Contact Center Management, you can give the user a Web Client user ID and password at the same time. In the **Supervisor Information** section, type the supervisor’s Web Client user ID and password.

Note:

Notes:

- Symposium Web Client user passwords can only contain English characters.
- After adding a Symposium Call Center Server supervisor or supervisor/agent as a Web Client user, you must still configure the user in the Access and Partition Management component. For example, you must still assign the user basic access rights to the different components, access classes, partitions, and supervisor/reporting agents.

To enable this supervisor to see all of his or her own reporting agents, In Access and Partition Management, assign the corresponding Web Client user profile

- the applicable supervisor/reporting agent combination (his or her reporting agents)
- a partition

For more information, see the “Supervisor/reporting agents feature” on page 464.

More information

For more information, refer to the *Symposium Call Center Web Client Supervisor’s Reference Guide*, or refer to the step-by-step procedures in the online Help.

Using the XML automated assignments feature

Introduction

Note: For information on installing this feature, see the *XML Assignments User Guide*. This guide, and other associated documentation and engineering/ development support resources for the XML automated assignments feature, are provided only through the Nortel Networks Developer Program. For information on obtaining the XML Automated Assignment toolkit, contact a member of the Developer Program through the Contact Us link on their web site at http://www.nortelnetworks.com/developer. General information on the Developer Program, including an online membership application, is also available on this site.

The XML automated assignments feature includes a Component service that can help you create or update multiple assignments simultaneously by parsing through assignment data located in XML files that you create. After the service parses the data, it either creates a new assignment on the indicated server, or it updates an existing assignment (if the assignment name in the XML file matches an existing assignment name on the selected server in Symposium Call Center Server).

When you create the XML file, you can specify whether you want the service to create an ad hoc assignment (one that is run immediately), or a scheduled assignment. If it creates a *new* scheduled assignment, then you must use the Contact Center Management component to manually schedule and activate the assignment; if it updates an *existing* scheduled assignment, then the schedule still applies and the assignment is still active. However, note that if you want the assignment to run only at the scheduled time, then you must select the *Schedule* option in the XML file. If you choose the *Execute Now* option, then the scheduled assignment will run twice: it will run immediately and at the scheduled time. If you do not include the <*EXECUTENOW*> field in your XML file, or if you type an invalid value in this field, then the system defaults to scheduling the assignment, and you must use Contact Center Management to manually schedule the new assignment.

Note: This feature does not include an interface for writing the XML files. Instead, you must create the files using a proprietary tool of your choice, designed to the specifications listed in “Specifications for XML files” on page 431. For guidance on creating the XML files, you can view the sample files that are shipped with the Symposium Web Client software. These files are located on the application server in the folder *C*:\Program Files\Nortel Networks\WClient\Server\XMLAssignments\Sample XML Files, where *C* is the drive on which you installed Symposium Web Client.

Prerequisites

Before you can use this feature, you must

- install it manually. For more information, see the *XML Assignments User Guide*. This guide, and other associated documentation and engineering/ development support resources for the XML automated assignments feature, are provided only through the Nortel Networks Developer Program. For information on obtaining the XML Automated Assignment toolkit, contact a member of the Developer Program through the Contact Us link on their web site at http://www.nortelnetworks.com/developer. General information on the Developer Program, including an online membership application, is also available on this site.
- be familiar with creating XML files. This feature does not include an interface for creating the XML files. However, it does include an XML schema. This file describes the format in which you must generate the files using the tool of your choice—either a Work Force Management (WFM) system or another third-party application—so that they can be interpreted by this feature. The file is called SWCXMLAssignments.xsd and is located in the following folder on the application server: *C*:\Program Files\Nortel Networks\WClient\Server\XMLAssignments, where *C* is the drive on which you installed Symposium Web Client.

Limitations

This section lists the maximum number of agent to skillset and agent to supervisor assignments that you can set up and schedule to run concurrently using this feature.

Supervisor assignment limits

You can create an agent to supervisor assignment that contains a maximum of 1000 entries, where assigning an agent to a supervisor is considered an entry. Nortel Networks recommends that you do not run multiple supervisor assignments concurrently.

Skillset assignment limits

You can create an agent to skillset assignment that contains a maximum of 1000 entries, where assigning an agent to a skillset is considered an entry and where the number of skillsets times the number of agents involved is less than 5000. Nortel Networks recommends that you do not run multiple skillset reassignments concurrently.

Generally, Nortel Networks recommends that you do not reassign more than 2500 entries per hour, a figure is based on operational experience. However, due to the broad spectrum of processor speeds and the diversity of call centers, this value is a guideline rather than a strict limit.

Overview of steps

The XML automated assignments feature involves the following general steps:

1. You create separate XML files for agent to supervisor and agent to skillset assignments using the tool of your choice (for example, a WFM system).
2. You place the XML files in the designated drop folder. This is the folder that you specified during the installation of the XML automated assignments feature. If you did not choose a specific folder, then place the files in the default folder: *C*:\Program Files\Nortel Networks\WClient\Assignments\XMLAssignments, where *C* is the drive on which you installed Symposium Web Client.
3. When you place a file in this folder, the service automatically detects it and parses through the file. If you have specified a new assignment name in the file, then the program creates a new assignment on the server in Symposium Call Center Server that you indicated in the file. If you specified an assignment name that already exists on the selected server, then the program updates the existing assignment with the new details.
4. After it parses through the file, the service deletes it from the drop folder, thus ensuring that only new files are parsed.

5. If you have created a new ad hoc assignment and have specified for it to *Execute Now,* then the assignment runs immediately. If you have created a *new* scheduled assignment, then you must schedule and activate it using the Contact Center Management interface. You can set the new assignment to run ad hoc by specifying *Execute Now* within the XML file, or schedule it to run on a recurring basis using Contact Center Management.

   Note: New scheduled assignments created with the XML automated assignments feature do not run until you activate and schedule them in the Contact Center Management component. However, if you update an *existing* activated and scheduled assignment by this means, then the schedule is still intact and the assignment is still activated. Note that if you want the assignment to run only at the scheduled time, then you must select the *Schedule* option in the XML file. If you choose the *Execute Now* option, then the scheduled assignment will run twice: it will run immediately and at the scheduled time. If you do not include the <*EXECUTENOW*> field in your XML file, or if you type an invalid value in this field, then the system defaults to scheduling the assignment, and you must use Contact Center Management to manually schedule the new assignment.

6. If the service encounters errors in the XML file that you have created, then it stops parsing the file, does not create or update the assignment, and it moves the file to the designated drop folder for problem files. If you did not choose a specific location for problem files during the installation, then the program places the files in the default location: *C*:\Program Files\Nortel Networks\WClient\Assignments\XMLAssignmentError, where *C* is the drive on which you installed Symposium Web Client. The system notifies you of problem assignments in the Audit Trail component.

   Note: The program also rejects files that contain more than 1000 entries notifies you of rejected assignments in the Audit Trail component. An example of an entry is assigning an agent to a supervisor or to a skillset. To prevent your files from being rejected, therefore, limit each file to 1000 entries or less. For more information, see “Limitations” on page 427.

7. If the service has rejected the XML file you have created, fix the problem and place the file in the drop folder to be parsed again. Continue this process until the service successfully parses the file and creates or updates the assignment. Then, schedule and activate the assignment in Contact Center Management, if required.

Who should use this feature

This feature is designed for large call centers in which, regardless of the number of skillsets associated with an agent, only one skillset is active at any time or in any physical location in the call center.

Some possible scenarios where this feature can be used follow:

- An agent is assigned to three skillsets during normal traffic periods, but during busy hours, you can use the XML automated assignments feature to assign this agent to additional skillsets.
- An agent may be in Standby mode for certain skillsets during non-peak times. However, during busy periods, you can use this feature to schedule an assignment that gives the agent a priority for these skillsets. You can run a second assignment later to put the agents into Standby mode again.
- An agent answers calls in the morning and in the afternoon, is in training, meetings, or does other work. You can use this feature to place these agents in Standby mode in the afternoon. You can also use this feature in cases where agents handle voice calls in the morning and then, in the afternoon, handle e-mail, web requests, and so on.

Example

Your call center has 500 agents, each of whom rotates daily in free seating mode within his or her team, with the skillset changing according to the seat the agent occupies.

In this example, agent John Smith works with skillsets S1, S2, and S3. On Monday morning, he works in area 1 (dedicated to skillset S1), in the afternoon, John works in area 2 (dedicated to S2), on Tuesday he works in area 3 (dedicated to S3), and so on.

You must create separate XML files—different files for agent to skillset and agent to supervisor assignments—that contain the assignment data for all 500 agents and their supervisors for each seat rotation period. In this scenario, therefore, you create separate agent to supervisor and agent to skillset assignment files for the Monday morning period, new files for the assignments on Monday afternoon, more files for Tuesday morning, and so on.

Once you create the files and are satisfied that they conform to the standards listed in the section “Specifications for XML files” below, you must copy them to the designated drop folder. When you place the files in this folder, the program automatically parses through the assignment data and creates or updates the assignment for all 500 agents. If you are creating new scheduled assignments, then you must use Contact Center Management to schedule and activate the assignments. If you are updating existing scheduled and activated assignments, then the assignments still use the same schedule and you do not need to use Contact Center Management.

Specifications for XML files

Valid XML files must contain the following data items for the service to parse them successfully:

- **Version** The service uses the version field to identify the XML Schema version used by the XML file.
- **Assignment name** This is an alphanumeric data field that identifies the name of the assignment to be created or updated. This data is enclosed within the XML tags `<ASSIGNMENTNAME> </ASSIGNMENTNAME>`.
- **Execute option** This is an optional field that enables you to specify whether you want to run the assignment immediately by typing the value **Execute Now**. If you want to save and schedule a new assignment in Contact Center Management, or if you want to update an existing scheduled assignment, then you can type the value **Schedule** in this field. (If you do not include this field in your XML file, or if you type an invalid value in this field, then the system defaults to scheduling the assignment, and you must use Contact Center Management to manually schedule the new assignment.) The value you choose is enclosed within the XML tags `<EXECUTEOPTION> </EXECUTEOPTION>`.
- **Symposium Call Center Server IP address** This is an alphanumeric field used to identify the server in Symposium Call Center Server on which the assignment is to be created or updated. Type the IP address of the server in Symposium Call Center Server on which you want to create the assignment. This data is enclosed within the XML tags `<IPADDRESS> </IPADDRESS>`.
- **Agent details** The agent details section contains data that uniquely identifies an agent (for example, the agent’s first name, last name, and

phoneset login ID). In this section, the first name and last name data is optional; the login ID is mandatory. This data is enclosed within the following XML tags:

```
<AGENT>
     <FIRSTNAME> </FIRSTNAME>
     <LASTNAME> </LASTNAME>
     <LOGINID> </LOGINID>
</AGENT>
```

- **Skillset details** The skillset details contain the skillset name and priority for the agent to skillset assignment. This data is enclosed within the following XML tags:

```
<SKILLSET>
     <NAME> </NAME>
     <PRIORITY></PRIORITY>
</SKILLSET>
```

The XML skillset tag <SKILLSET> is embedded within the agent XML tag <AGENT> for each skillset that is assigned/unassigned to an agent, as shown below. In this section, the first name and last name data is optional; the rest of the data is mandatory.

```
<AGENT>
     <FIRSTNAME> </FIRSTNAME>
     <LASTNAME> </LASTNAME>
     <LOGINID> </LOGINID>
     <SKILLSET>
          <NAME> </NAME>
          <PRIORITY> </PRIORITY>
     </SKILLSET>
     <SKILLSET>
          <NAME> </NAME>
          <PRIORITY> </PRIORITY>
```

```
        </SKILLSET>
        ..............
        ..............
    </AGENT>
```

- **Supervisor details** The supervisor details section contains data that uniquely identifies the supervisor to whom the agent is to be assigned. In this section, the name data is optional; the ID is mandatory.This data is enclosed within the following XML tags:

```
<PRIMARYSUPERVISOR>
    <ID> </ID>
    <NAME> </NAME>
</PRIMARYSUPERVISOR>
```

The supervisor XML tag <SUPERVISOR> is embedded within the agent XML tag <AGENT>. The supervisor tag appears once within the agent tag for each agent to supervisor assignment, as shown below. In this section, the agent first name, last name, and primary supervisor name data is optional; the login ID and ID values are mandatory.

```
<AGENT>
    <FIRSTNAME> </FIRSTNAME>
    <LASTNAME> </LASTNAME>
    <LOGINID> </LOGINID>
      <PRIMARYSUPERVISOR>
        <ID> </ID>
        <NAME> </NAME>
      </PRIMARYSUPERVISOR>
</AGENT>
```

What's next?

After you create assignments in Contact Center Management, create report groups, partitions, and access classes in the Access and Partition Management component. Then you can create Web Client users, and assign them basic access rights, partitions, access classes, and supervisor/reporting agent combinations.

Section D: Access and Partition Management

In this section

Overview	436
Creating report groups	441
Creating partitions	444
Creating access classes	453
Adding and configuring users	462
Supervisor/reporting agents feature	464

Overview

Introduction

You can use the Access and Partition Management component to create Web Client users and assign them the appropriate access privileges to the system. Web Client users can log on to the application server and use the Symposium Web Client components to which they have been given access. You can control their access privileges by assigning these users basic access rights, access classes, partitions, and supervisor/reporting agent combinations.

Note: To add a Symposium Call Center Server user (agent, supervisor, or supervisor/agent), you must use the Contact Center Management component, or use the spreadsheet in the Configuration component. Some Symposium Call Center Server users (supervisors and supervisor/agents) may also be Web Client users and be given a Web Client user ID and password to access the application server; however, many Symposium Call Center Server users will never use Symposium Web Client.

You can use Access and Partition Management to add, edit, view, or delete

- Symposium Web Client users
- partitions
- access classes
- report groups for Historical Reporting
- basic access rights to different Symposium Web Client components

Access rights, access classes, partitions, and supervisor/reporting agent combinations

There are four mechanisms in Symposium Web Client that you can use to control the data that users can access in the call center:

- basic access rights to each component in Symposium Web Client
- access classes
- partitions
- supervisor/reporting agent combinations

Access rights

The most basic level of security is the overall right to access the components within Symposium Web Client. When you add Web Client users in Access and Partition Management, you can specify which components the users can access. If you do not grant a user basic access to a component, then the component is not visible to the user on the Symposium Web Client launchpad.

Access classes

Access classes allow you to control the actions (for example, none, read only, read/update, read/update/create/delete) that users can perform when configuring the call center while using the Contact Center Management, Configuration, and Scripting components.

Note: Access classes are not defined for any of the remaining Symposium Web Client features. To perform all functions in these components, users require only basic access rights.

Partitions

Partitions allow you to specify which data Web Client users can view and manage on a per-server basis in Real-Time Reporting, Historical Reporting, and Contact Center Management. After you grant users basic access rights to these components, you can control the data they can access on each server by adding the data elements to the partition assigned to the users. You can, for example, give a user access to data on only one server in the network.

Supervisor/reporting agent combinations

Similar to a partition containing only agents, this feature enables you to link supervisors (and all their reporting agents) to a Web Client user on a per server basis. For a Web Client user who is also a supervisor, you can link the two profiles, ensuring that the supervisor automatically sees all his or her agents in the historical reports, real-time displays, and in Contact Center Management. Unlike partitions in which you can choose individual agents, in the supervisor/ reporting agent feature, you cannot specify the particular agents that a user can see; once you associate a Web Client user with a supervisor, then the user automatically sees *all* the supervisor's reporting agents.

Note: In most cases, the supervisor/reporting agents feature only works in conjunction with partitions: you must assign both a partition and a supervisor/reporting combination to a user to restrict the user to seeing his or her reporting agents. The exception to this rule is in Real-Time Reporting, specifically for the private agent real-time displays and agent map displays. If you have assigned the user *only* a supervisor/reporting agent combination in Access and Partition Management (not a partition), then the user can apply this supervisor/reporting agent combination to either a private agent real-time display, or an agent map display to view only those reporting agents. For more information, see Appendix E, “Supervisor/reporting agents matrix.”

Together, these four features allow you to tailor access rights to suit every user in the call center.

Example

You first grant a user general access to Contact Center Management. Then you define the actions the user can perform in Contact Center Management. For example, you can give the user *Edit Agent and Supervisor Properties* access in CCM. Finally, you specify the data that the user can see in Contact Center Management by defining a partition containing the appropriate agents and assigning it to that user, or by assigning *both* a partition and one or more supervisor/reporting agent combinations to the user.

When the user opens the Contact Center Management component, he or she can see only the agents specified in the partition, or the agents reporting to the supervisor associated with this user (or both), and can edit, read, and update agents and supervisors. For more information about the Contact Center Management access classes, see the online Help included with the application.

Security level	Resulting example
Grant overall access rights to individual components for the user.	Access to Contact Center Management.
Define an access class for the user.	*Edit Agent and Supervisor Properties* access in CCM.
Define a partition with various data.	A partition with agent data.

Security level	Resulting example
Assign that partition to the user, or assign the user both a partition and a supervisor/reporting agent combination.	When the user opens the Contact Center Management component, he or she sees only the agents specified in the partition, or the agents in both the partition and supervisor/reporting agent combination, and can edit, read, and update agents and supervisors.

ATTENTION

If you do not assign a partition to a user, then that user can see *all* data pertaining to the call center in Historical Reporting and Contact Center Management on each server in the network, regardless of whether you assign the user a supervisor/reporting agent combination. This is assuming that the user has been given basic access rights to these components.

In Real-Time Reporting, however, the data the user can see varies based on the type of display the user opens and whether the user has been assigned a partition or a supervisor/reporting agent combination (or both). For more information, see Appendix E, “Supervisor/reporting agents matrix.”

Creating report groups, partitions, and access classes

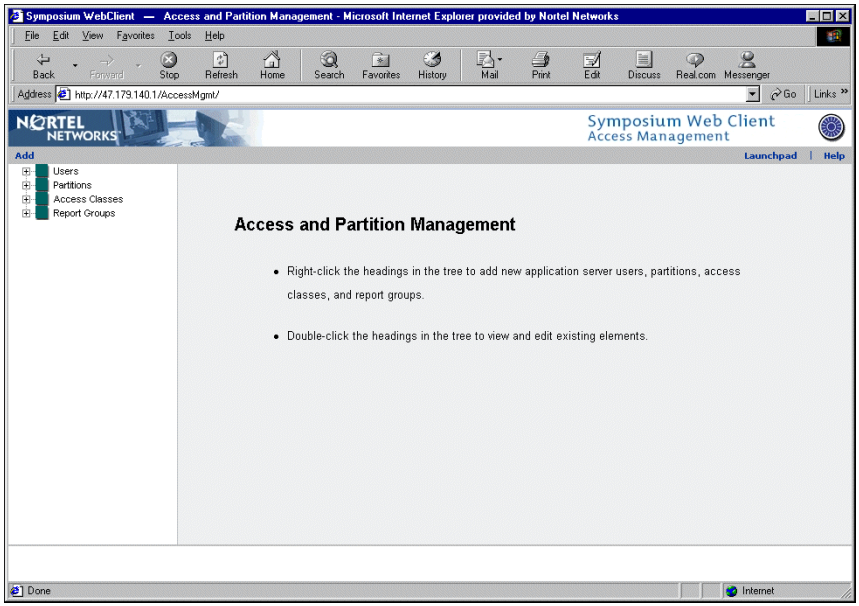
This section provides a high-level overview of the following tasks:

- creating report groups
- creating partitions
- creating access classes

Note: After you perform these tasks, you must add and configure Web Client users. When you configure Web Client users, you assign them basic access rights, partitions, access classes, and supervisor/reporting agent combinations. For more information, see “Adding and configuring users” on page 462.

After clicking Access and Partition Management from the launchpad, click **Add** from the toolbar in the Access and Partition Management main window to add report groups, partitions, access classes, and Web Client users.

Access and Partition Management main window



For detailed step-by-step procedures about using the Access and Partition Management component, see the Symposium Web Client online Help.

Creating report groups

Introduction

Since report groups are added to partitions, you may want to create the report groups before you define the partitions and assign them to users.

There are two categories of report groups in Historical Reporting:

- **Public report groups** These report groups contain the standard public report templates. The six public report groups are Agent Performance, Configuration, Call-by-Call, Networking (only networking versions of the M1/CSE 1000/M1 IE switches), Others, and NCC (on the NCC only).

Note: The current release of the CSE 1000 switch only supports networking over ISDN trunks.

- **Custom report groups** These report groups contain the report templates that users belonging to the group have customized and want to share with other members of the report group. The custom report groups that you create in this window are for use in Historical Reporting. You can assign any unique name to these groups.

Public report groups versus Custom report groups

Unlike the *public* report groups that contain all of the standard templates, *custom* report groups do not contain any standard templates. The custom report groups that you create in Access and Partition Management are folders that enable Historical Reporting users who belong to the same group to share their customized reports. Users can customize a standard template and save it in their group folder so that other group members can use the same customized report.

You can create *custom* report groups to reflect each department in your call center, such as the Sales Group or the Marketing Group. If you are configuring a shared call center, you can also create separate groups for each company sharing the call center, such as the Best Air Group and the Econo Air Group. In this way, you can keep customized reports that contain company information separate from other companies in the same call center.

Note: The data shown in each report is based on the partitions assigned to the user and the selection criteria the user applies to the report.

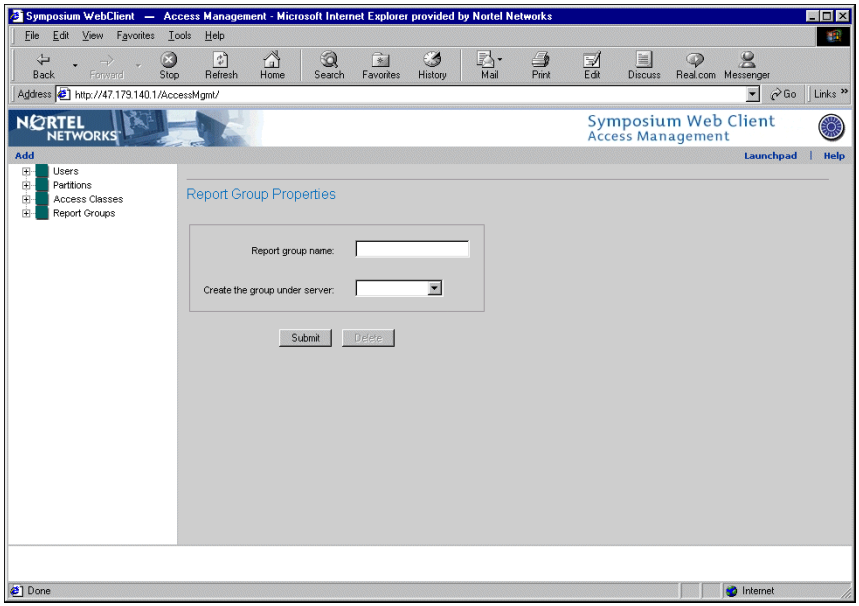
Report groups also enable you to grant a user access to a very limited number of reports. For example, if you do not want to give a user access to any of the standard report templates, you can create a custom report group and add it to the partition assigned to the user. When the user opens Historical Reporting, he or she sees only the custom report group folder, and can only see reports that other members of the group have saved in the group folder.

After you create a report group, you must add it to a partition created under the *same server* as the report group. Then you must assign the partition to the users belonging to the report group. When these users log on to Symposium Web Client, they see the report group name in Historical Reporting under the server where you created it.

To add a new report group, select Add → New Report Group from the toolbar in the Access and Partition Management main window.

Note: Do not use the ampersand symbol (&) in the report group name.

Report Group Properties window



Once you name the Report Group and identify the server to which you are adding the Report Group, click **Submit**. The new Report Group appears on the system tree under Report Groups.

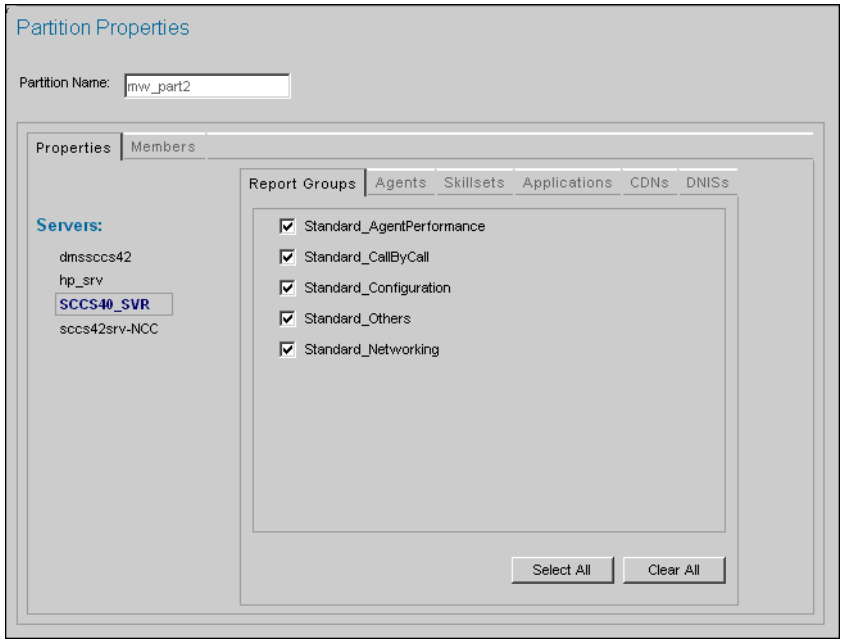
Creating partitions

Introduction

To create a new partition, select Add → New Partition from the toolbar in the Access and Partition Management main window.

Note: Do not use the ampersand symbol (&) in the partition name.

Partition Properties window



Notes:

- Click the **Members** tab to view the list of users who are currently assigned the partition.
- To give users access to data on more than one server in your network, you can create a partition that spans multiple servers. However, note that when doing so, you must choose the partition properties on each server for the user to be able to see the data on these servers. For example, to enable a

user to see agents configured on two servers, you must select this agent on each server individually when configuring the partition. If you only choose elements on one server for the partition, then the users assigned the partition can only see the data on this one server.

- If there are a large number of agents configured on the server, you may have to wait a few moments while the system retrieves the agent data and populates the Agent tab.

Partition properties

When you create a partition, you can specify the following types of data:

- report groups
- agents
- skillsets
- applications
- CDNs
- DNISs

When you assign a partition to a user that contains all six types of data, the user sees either all of the data types in the partition, or a fraction of them, depending on the Symposium Web Client component that the user is using. The Symposium Web Client components are each designed to allow users to work with particular types of data. For example, Contact Center Management is strictly for configuring and managing call center supervisors, agents, and for assigning agents to skillsets; therefore, the only partition elements that appear in Contact Center Management are agents and skillsets.

If you do not include certain types of data in a user's partition, then the user does not see this data. For example, if you do not include CDNs and DNISs in the user's partition, then the user sees no CDNs or DNISs in Historical Reporting.

Note: Users are restricted to viewing their partitioned skillsets in Contact Center Management only if you assign to them an access class containing the *Use Agent & Skillset Partitions in CCM* access level. If you do not assign this access level to the user, then he or she sees all configured skillsets in Contact Center Management, regardless of whether they are included in their partition.

If you assign a partition containing all six elements to a user, the user sees the following elements in each of the Web Client applications:

Component	Types of data available in the partition
Historical Reporting	■ skillsets ■ agents ■ applications ■ CDNs ■ DNISs ■ report groups
Real-Time Reporting	■ skillsets ■ agents ■ applications
Contact Center Management	■ agents ■ skillsets* * Only if you assign the *Use Agent & Skillset Partitions in CCM* access level to the user. Otherwise, the user sees all configured skillsets in Contact Center Management, regardless of whether there are skillsets in the partition.

A partition can contain any combination of the six elements, but it does not have to contain all elements. For example, it can contain only skillsets and agents, but not CDNs, DNISs, applications, or report groups.

After you create the partition, you must assign it to the appropriate Symposium Web Client users. Once you assign the partition, the user can view the partitioned data in the real-time displays, historical reports, and in Contact Center Management.

ATTENTION

If you do not assign a partition to a user, then that user can see *all* data pertaining to the call center in Historical Reporting, Contact Center Management, and in the public agent real-time displays in Real-Time Reporting on all servers in the network, regardless of whether you have assigned a supervisor/reporting agent combination to the user. The private agent real-time displays and agent map graphical displays behave differently than the public displays. For more information, see Appendix E, "Supervisor/reporting agents matrix."

- If you *only* assign the user a partition, then keep in mind that users cannot see data that is not included in their partition. Therefore, when you add an agent in Contact Center Management, you must also add the agent to the user's partition to enable the user to see the agent in the real-time displays, historical reports, and in Contact Center Management.
- However, if you assign the user *both* a partition and a supervisor/reporting agent combination, then you do not have to update the user's profile when you add a new agent who is assigned to the user; the supervisor/ reporting agent combination is automatically updated as new agents are added and, therefore, always includes all agents assigned to the supervisor. For more information, see the "Supervisor/reporting agents feature" on page 464.

Agent partitions and supervisor/reporting agent combinations

In addition to assigning a Web Client user a partition, you can assign the user a supervisor/reporting agent combination. The supervisor/reporting agents feature is similar to agent partitions, but it only works in conjunction with partitions (except in the case of private agent real-time displays and agent map displays, in which case, partitions are not mandatory).

If you do not assign a partition to a user, then that user can see *all* data pertaining to the call center in Historical Reporting, Contact Center Management, and in the public agent displays in Real-Time Reporting on all servers in the network, regardless of whether you have assigned a supervisor/reporting agent combination to the user. For the private agent real-time displays and agent map displays, however, if you assign the user only a supervisor/reporting agent combination (not a partition), then the user can assign this combination to the display (just as they would apply a custom filter), to view only those reporting agents on the display. Partitions are not required to limit the agents the user sees in these types of displays. For more information, see the "Supervisor/reporting agents feature" on page 464, and Appendix E, "Supervisor/reporting agents matrix."

Note: If there are a large number of agents configured on the server, when you click the Agent tab, you may have to wait a few moments while the system retrieves the agent data and populates the tab.

When you assign a Web Client user a partition containing agents, it is similar to assigning the user a supervisor/reporting agent combination, except for the differences outlined in the following table.

Partitions containing agents	Supervisor/reporting agent combination
You can customize partitions.	You cannot customize supervisor/ reporting agent combinations.
■ You can specify which agents you *want* the Web Client user to see, on a per server basis.	■ When you assign a Web Client user a supervisor/reporting agent combination, you automatically grant the user access to *all* the supervisor's reporting agents, on a per server basis.

Partitions containing agents	Supervisor/reporting agent combination
Partitions are not dynamic. ■ When you assign a new agent to a supervisor, you must manually update the partition assigned to the supervisor (the Web Client user) to include the new agent.	Supervisor/reporting agent combinations are dynamic. ■ When you assign a new agent to a supervisor, the corresponding supervisor/reporting agent combination is automatically updated to include the new agent. Any Web Client users who have this supervisor/reporting agent combination assigned to them automatically have access to this new agent.

Example

Based on your call center configuration, you may want to use a combination of partitions containing agents and supervisor/reporting agent combinations. For example, you may want to enable a user to always see his or her reporting agents plus three other agents who are not assigned to the user (so that he or she can act as the associated supervisor for these agents). In this case, you assign the user a partition containing the three *associated* agents and the supervisor/reporting agent combination containing the user's own agents.

To see an example of how you would configure a Web Client user and assign him or her partitions, supervisor/reporting agent combinations, and other features, such as access classes and report groups, see "Sample task flow for configuring Web Client users" on page 475.

Partitions in Historical Reporting, Real-Time Reporting, and Contact Center Management

Note: This section only includes information on partitions; it does not include details on the supervisor/reporting agents feature. For more information on this feature, see the "Supervisor/reporting agents feature" on page 464.

Users are restricted to viewing only the types of data included in the partition assigned to them. (However, users can see *all* data if they are not assigned a partition.) For example, if you assign a partition to a user that only contains report groups, then that user sees no data in Real-Time Reporting or Contact Center Management because report groups do not apply to either of these components. Likewise, in Historical Reporting, this same user sees the report groups included in the partition, but does not see any data because only report groups are included in the partition assigned to the user.

Therefore, when you create and assign a partition to users, you must consider the types of data that these users have to monitor in the real-time displays, historical reports, and in Contact Center Management.

Notes:

- If you do not assign a partition to a Historical Reporting user, then the user automatically has access to all data *and* all public report templates (the standard report templates included with Symposium Web Client).
- If you do not assign a partition to a Real-Time Reporting user, then the user sees all data in the real-time displays, assuming that the user has been given basic access rights to this component.
- If you do not assign a partition to a Contact Center Management user, then the user sees all data in the Contact Center Management windows to which he or she has been given access.

Partitions and selection criteria in Historical Reporting

In Historical Reporting, if users do not choose the data elements they want to see in a report by defining the selection criteria, then the generated report automatically includes all the data in the user's partition that is applicable to the report type. For example, if the user generates an Agent Performance report and does not select any agents, the report includes all agents in the user's partition.

The exception to this rule occurs when

- the partition contains more than 250 data elements of a particular type (for example, more than 250 agents)
- the user does not define the selection criteria

In Symposium Web Client, users can select a maximum of 250 elements to include in the report. However, when they do not make a selection, and when the partition contains more than 250 data elements, the generated report contains *all* data configured in the system, including data outside the partition.

If the partition contains 250 agents or less, and the user does not define the selection criteria, then the report contains only the agents in the user's partition.

It is recommended, therefore, that administrators remind Web Client users to define the selection criteria before generating reports. If the user wants to view more than 250 elements in the report, then Nortel Networks recommends that he or she generate more than one report, defining the selection criteria for each report separately.

Partitions and filters in Real-Time Reporting

In Real-Time Reporting, users can specify the data that they want to see in their private real-time displays and the agent map graphical displays by creating filters and assigning the filters to the display. However, this option is available to users only if you have assigned a partition to them. Users who do not have partitions cannot create filters in Real-Time Reporting.

Partitions in Contact Center Management

In Contact Center Management, you can control the agents users see by adding them to a partition and assigning it to the appropriate users. Optionally, you can also control the skillsets that Contact Center Management users see by adding the skillsets to the partition assigned to the users, and then assigning these users an access class containing the *Use Agent & Skillset Partitions in CCM* access level. If you do not assign this access level, then users see all configured skillsets in Contact Center Management, regardless of the skillsets in their partitions.

Partitions and your call center

Partitions are especially useful when competing companies share the same call center. In the following example, the two companies that share the call center are Best Air and Econo Air.

To grant users access to data pertaining only to their company, administrators can create partitions within the call center and assign the partitions to different users, thereby restricting the view of the call center data that each user has.

For example, at a Toronto call center, there are 18 skillsets, 10 of which apply to agents answering calls for Best Air, while the remaining 8 skillsets apply to agents answering calls for Econo Air. To divide the call center so that supervisors see only the call activity applicable to their company, the call center administrator creates the following two partitions at the Toronto site:

- The first partition contains the 10 Best Air skillsets and the agents that answer these calls.
- The second partition contains the 8 Econo Air skillsets and the agents that answer these calls.

After creating these partitions, the call center administrator assigns them to the appropriate supervisors. When the supervisors view the Real-Time Reporting displays or the historical reports, they see only those elements in the partitions to which they belong.

Note: Partitions can only restrict one element at a time. For example, when a user runs a Skillset by Agent Performance report, he or she can choose to view agents from among those included in their partitions. However, sometimes an agent in the user's partition may be assigned to a skillset that is outside the user's partition. If a call is routed to an agent for a skillset that is not included in the user's partition, then the call statistic (and possibly the skillset details) appear in the Skillset by Agent Performance report.

Partitions are also useful if you want to separate your call center into different departments within the same company. For example, the administrator can create separate partitions for the Sales and Marketing departments, and assign each partition to supervisors working in each department.

Note: If an administrator does not assign a partition to a user, then that user can see all data pertaining to the call center in Real-Time Reporting, Historical Reporting, and Contact Center Management. In this example, therefore, if the administrator does not assign a partition to the supervisors, then the real-time displays, historical reports, and all windows in Contact Center Management to which the user has access contain all data configured on the selected server.

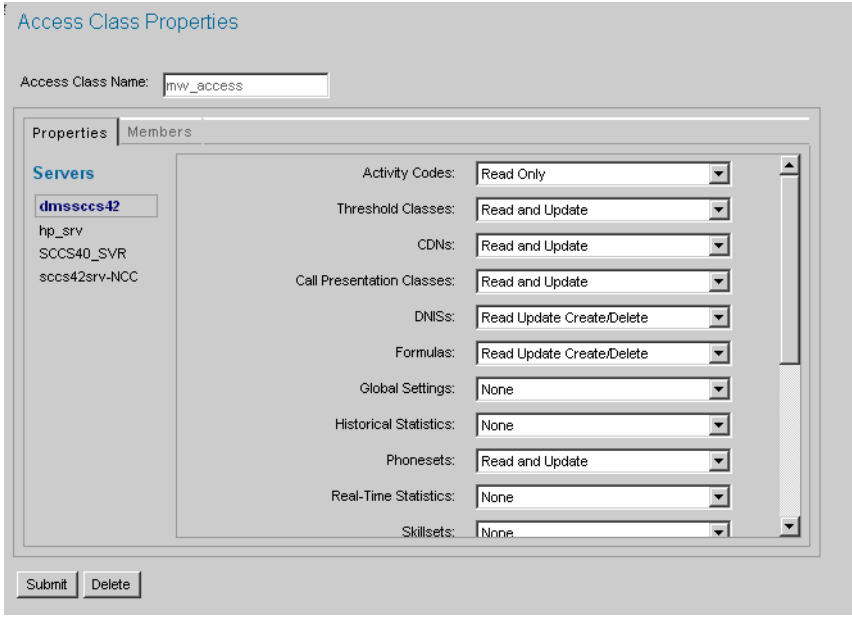
Creating access classes

Introduction

To create a new access class, select Add → New Access Class from the toolbar in the Access and Partition Management main window.

Note: Do not use the ampersand symbol (&) in the access class name.

Access Class Properties window



When you create a new access class, use a descriptive name for the type of user who will have this access level, or the type of privileges available at this access level. Once you type the name for the new access class, you must select each of the servers on which you want to create the access class. The server's access class elements appear.

Notes:

- You create an access class that spans multiple servers (if you work in a network), but you must choose the access class properties on one server before selecting the next server.
- The access class settings for all properties default to *None* for each server, except the CCM Partitions access class heading, which defaults to *Use Agent Partitions in CCM*.
- To grant access on all servers in your network, you must configure each server shown in the list of servers.
- When you grant a user access privileges that span multiple servers, the user only needs to log on to one server–the application server–to access all servers included in the access class. Users no longer need to log on to each individual server to which they have access.
- Click the **Members** tab to view the list of users who have been assigned the access class.

Selecting access levels within access class elements

In the Access Class Elements section, you select the access levels for the elements that you want to make available to this access class. The access class elements shown correspond to three Symposium Web Client components: Configuration, Scripting, and Contact Center Management. Users do not require an access class to work in any other component, but instead, they only have basic access rights. For a complete description of the access class levels and the actions they enable users to perform, see the online Help.

Configuration access class elements

If you grant the user basic access to Configuration, you must also assign an access class to the user that includes at least one of the Configuration access class elements, such as skillsets or DNISs. If you do not assign the user an access class with at least one of these privileges on at least one server, then the user sees nothing in Configuration.

Scripting access class elements

If you grant the user basic access to Scripting, then you must also assign an access class to the user that includes at least one of the Scripting access class elements: Scripts, Script Variables, or Application Thresholds. If you do not assign the user an access class with at least one of these privileges on at least one server, then the user sees nothing in Scripting.

Contact Center Management access class elements

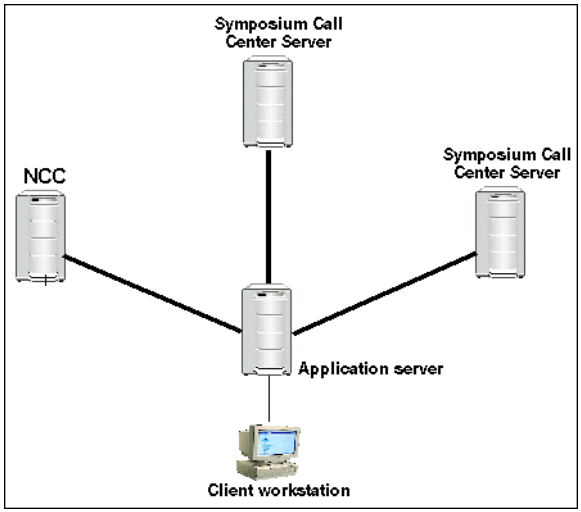
If you grant the user basic access to Contact Center Management, then the user can open Contact Center Management and see the opening window with the configured servers. However, to log on to the servers in each of the data views and work with data, the user requires the following access class levels:

- To log on to a server in agent view and see the agent details in all views, the user requires at least the *View Agent Properties* level of access under the CCM access class element on at least one server.
- To log on to a server in skillset view and view agent to skillset assignments, the user requires at least the *View Assignments* access level under the Skillset Assignment access class element.
- To log on to a server in supervisor view and view agent to supervisor assignments, the user requires at least the *View Assignments* access level under the Agent to Supervisor Assignment access class element.
- To log on to a server in assignments view and work with either agent to skillset or agent to supervisor assignments, the user requires at least the *Schedule Assignments* access level under either the Skillset Assignment or Agent to Supervisor Assignment access class elements (or both) on at least one server.

Access classes and servers

In Symposium Web Client, each access class that you create spans multiple servers (if you work in a multiple Symposium Call Center Server environment). However, you configure and manage the access classes by logging on to just *one* server—the application server, where access classes are stored.

The following diagram outlines a simplified network configuration for Symposium Web Client. When you log on to the application server from a client workstation, you can use the Access and Partition Management component to configure access classes for the servers in Symposium Call Center Server, and for the Network Control Center (NCC) server.



Each access class that you create spans all servers in the network, even if you do not select any access class elements on a particular server. For example, in the above network scenario, you create an access class that contains Configuration access elements only on the NCC server, and you assign it to a user. By not specifying any access elements on any other server in the network, you limit the user's actions on all servers, not just on the NCC server. This user does not have access to any of the Configuration elements on either of the servers in Symposium Call Center Server; the user can only perform the actions included in the access class to configure the NCC server.

If the user needs to configure either of the servers in Symposium Call Center Server, you must edit the user's access class to include access rights on the other servers.

Note: When you grant a user access privileges that span multiple servers, the user only needs to log on to one server–the application server–to access all servers included in the access class. Users no longer need to log on to each individual server to which they have access.

Defining typical call center administrator access

The following is an example of the access privileges that an administrator might have in a typical call center on at least one server in the network. He or she can do the following:

- Read, update, create, and delete all call presentation classes, skillsets, activity codes, phonesets, DNISs, routes, IVR ACD-DNs, CDNs, scripts and script variables, formulas, threshold classes, and all users, including supervisors. This user can also assign Web Client user IDs and passwords to the supervisors and supervisor/agents who need to log on to the application server and use Symposium Web Client (and then the administrator must finish configuring the new Web Client user profile in Access and Partition Management).
- View and assign all agents in agent to supervisor assignments and agent to skillset assignments.
- Create and run any report in Historical Reporting, and create and view all real-time displays.
- Edit all historical statistics, real-time statistics, and applications.
- View the status of Emergency Help requests.

To give a call center administrator these sample access privileges in Symposium Web Client, you must use a combination of two levels of security: basic access rights and access classes.

Note: To ensure that the administrator always has access to *all* data on the applicable server, do not assign the administrator a partition. If you do not assign a partition, the user automatically sees *all* available data. Conversely, to restrict the administrator's access to specific data, assign the administrator a partition containing only the applicable data on the appropriate server.

1. Create an administrator access class that contains read, update, create, and delete access for the following elements on the applicable server: call presentation classes, skillsets, activity codes, phonesets and voice ports, DNISs, routes, IVR ACD-DNs, CDNs, formulas, threshold classes, scripts, and script variables.

   This access class must also contain read and update access for historical statistics, real-time statistics, and application thresholds, as well as add, edit, delete agents and supervisors access in CCM, and schedule

assignments access under both the Agent to Supervisor Assignment and Skillset Assignment access class elements.

2. Create the administrator user profile in Access and Partition Management, and give the administrator basic access rights to all components in Symposium Web Client, except Access and Partition Management. (Users who have basic access to Access and Partition Management have overall administrative privileges, and can create and delete access classes, partitions, report groups, and Web Client users. There must be one administrator with this privilege in the call center network.)

   When you grant basic access to the remaining components of Symposium Web Client, you enable the administrator to create and run any report in Historical Reporting, create and view all real-time displays, and view the status of Emergency Help requests.

   Note: When you grant users basic access to Real-Time Reporting and Historical Reporting, they can access these components on all servers in the network. However, you can restrict the data that a user can view on each server by assigning a partition to the user. For example, if a user should not have Real-Time Reporting capabilities on one server, then you can assign a partition to the user that does not contain any data for that server. The user can still open the Real-Time Reporting component on that server, but cannot view any data in any of its real-time displays.

3. Assign the access class to the administrator.

If the administrator requires access privileges on more servers in the network, you can add the access privileges on the additional servers to the administrator's access class.

Defining typical supervisor access

The following is an example of the access privileges that a typical call center supervisor might have on one server in the network. He or she can do the following:

- View and edit agents and supervisors, and view and assign all agents in agent to supervisor assignments and agent to skillset assignments.
- Create and run agent performance reports in Historical Reporting.
- Create and view all real-time displays.

- View the status of Emergency Help requests.

To give a call center supervisor these access privileges in Symposium Web Client, you need to use a combination of up to four features: basic access rights, access classes, partitions, and, optionally, supervisor/reporting agent combinations.

1. Create a supervisor access class that contains edit agent and supervisor properties access for CCM, and schedule assignments access for both Agent to Supervisor Assignments and Skillset Assignments on the applicable server.

   This access class enables the supervisor to view and edit agents and supervisors, assign agents to partitions in Contact Center Management, view and assign all agents in agent to supervisor assignments and agent to skillset assignments, and schedule these assignments.

   Note: If you do not want to allow the supervisor to view and edit users, but only want to allow him or her to create ad hoc assignments, then the access class must contain *Ad Hoc Assignments* access for agent to supervisor assignments and agent to skillset assignments. It does not include any access level in the CCM access class element.

2. Create a partition on the appropriate server that contains all the supervisor's agents, the appropriate skillsets, applications, and the Standard Agent Performance report group.

   This partition enables the supervisor to work with his or her agents in Contact Center Management, view these agents, skillsets, and applications in the Real-Time Displays, and run any agent performance reports.

   Tip: Since partitions are not dynamic, whenever you assign an agent to a supervisor, you must update the partition assigned to the supervisor to include the new agent; otherwise, the supervisor will not see the agent in the real-time displays, historical reports, or in Contact Center Management. To avoid having to update the list of agents in the partition, you can use the supervisor/reporting agents feature, which enables you to associate the supervisor's Web Client user profile with his or her supervisor profile (which, in turn, is linked to all the supervisor's reporting agents). This association is dynamic, meaning that each time you assign an agent to the supervisor, the agent is automatically associated with the supervisor profile. In addition to this association, create a partition containing the appropriate

skillsets, applications, and the Standard Agent Performance report group. The combination of the partition and the supervisor/reporting agent association enables the supervisor to always have an up-to-date list of agents, and to view their skillsets and applications in the real-time displays and historical reports. For more information, see the “Supervisor/reporting agents feature” on page 464.

3. Create the supervisor user profile in Access and Partition Management and give the supervisor basic access rights to Real-Time Reporting, Historical Reporting, Contact Center Management, and Emergency Help.

   This enables the supervisor to have basic access to each of these components, create and view real-time displays (containing only the data included in their partition), create and run historical reports (only the agent performance reports included in their partition, and only with the partitioned agents, skillsets, and applications), and view the status of Emergency Help requests.

   Note: Partitions and supervisor/reporting agent combinations behave differently in Real-Time Reporting, based on the type of display the user opens and whether the user applies a supervisor/reporting agent combination or a filter to the display. For more information, see “Partitions and supervisor/reporting agent combinations in Real-Time Reporting” on page 470.

4. Assign the access class, the partition, and, optionally, the supervisor/reporting agent combination to the supervisor’s Web Client user profile.

If the supervisor requires access privileges on more servers in the network, you can add the access privileges on the additional servers to the supervisor access class.

To view an example of how you would configure a Web Client user and assign him or her partitions, supervisor/reporting agent combinations, and other features, such as access classes and report groups, see “Sample task flow for configuring Web Client users” on page 475.

Note: If you have included agents in the partition assigned to the supervisor, then whenever a new agent is assigned to the supervisor, you must add the agent to the supervisor’s partition so that the supervisor can monitor the agent in Real-Time and Historical Reporting, and can view the agent in Contact Center Management. You can avoid having to update the agents in the partition by

associating a supervisor/reporting agent combination with the supervisor's Web Client user profile. This association is dynamic, meaning that each time a new agent is assigned to the supervisor, the agent is automatically associated with the supervisor's user profile. For more information, see the "Supervisor/reporting agents feature" on page 464.

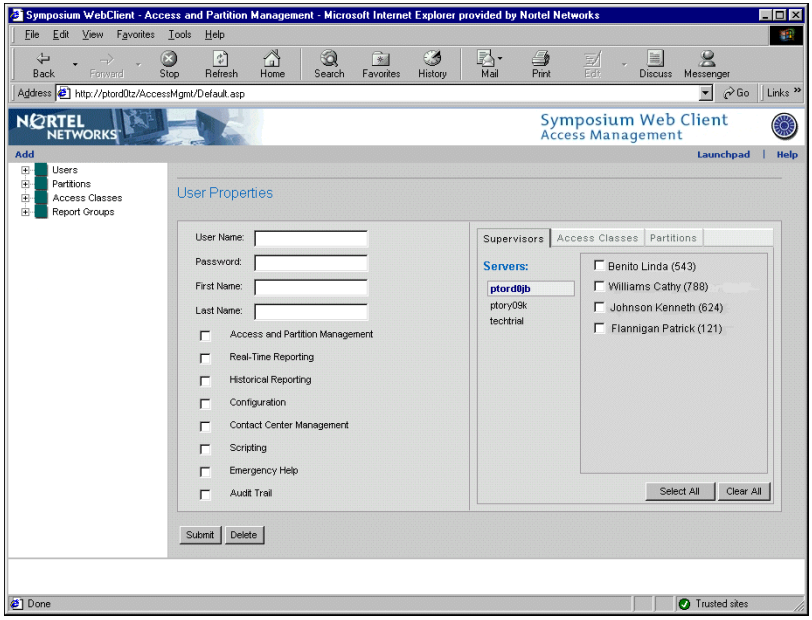
Adding and configuring users

Introduction

You create Web Client users in the Access and Partition Management component. To add a new Web Client user, select Add → New User from the toolbar in the Access and Partition Management main window.

Note: Do not use the ampersand symbol (&) in the user's name.

User Properties window



Assigning basic access rights, access classes, partitions, and supervisor/reporting agent combinations

When you define Web Client users, you assign to them

- basic access to the appropriate components within Symposium Web Client

- access classes that control the *actions* they can perform in these components (On the **Access Classes** tab, you can see the Access Classes that you created.)
- partitions and supervisor/reporting agent combinations that control the *data* they can see in these components (On the **Partitions** tab, you can see the partitions that you created, and on the **Supervisors** tab, you can see the list of all supervisors who are configured on each server in your network.)

ATTENTION

Once you create a user, you cannot modify the user name. You must delete the user and create a new user with the new name.

Users with Access and Partition Management access have administrator privileges in Symposium Web Client, enabling them to perform almost all administrative functions. However, only the default administrator, *webadmin*, can access and use the Configuration spreadsheets for uploading and downloading configuration data, and can add, edit, and delete servers in Configuration.

To view an example of how you would configure a Web Client user and assign him or her partitions, supervisor/reporting agent combinations, and other features, such as access classes and report groups, see “Sample task flow for configuring Web Client users” on page 475.

Supervisor/reporting agents feature

Introduction

The supervisor/reporting agents feature enables you to dynamically link a supervisor and all his or her reporting agents with one or more Web Client users, thereby enabling the users to view the agents in Symposium Web Client components, such as Real-Time and Historical Reporting, and Contact Center Management. You assign supervisor/reporting agent combinations to Web Client users by using the **Supervisors** tab in the User Properties window of Access and Partition Management.

Notes:

- Partitions and supervisor/reporting agent combinations behave differently in Real-Time Reporting, based on the type of display the user opens and whether the user applies a supervisor/reporting agent combination or a filter to the display. For more information, see “Partitions and supervisor/ reporting agent combinations in Real-Time Reporting” on page 470. For a detailed listing of how this feature works in conjunction with partitions in each of the Symposium Web Client components (Real-Time and Historical Reporting and Contact Center Management), see Appendix E, “Supervisor/ reporting agents matrix.”
- In most cases, the supervisor/reporting agents feature only works in conjunction with partitions, that is, you must assign the user *both* a partition and a supervisor/reporting agent combination for the user to see all his or her reporting agents (and any agents in the partition). If you do not assign the user a partition, but only a supervisor/reporting agent combination, then the user sees *all* agent data. Private agent real-time displays and agent map displays are the exception to this rule. For details, see Appendix E, “Supervisor/reporting agents matrix.”

Tip: To enable the user to always see *only* his or her reporting agents, assign the user a partition that does not contain any agents and the appropriate supervisor/ reporting agent combination. This way, you do not have to manually update the partition as new agents are assigned to the user because the supervisor/reporting agent combination automatically reflects all new agents. Note however, that only partitions (and not supervisor/reporting agent combinations) are applicable to

standard real-time displays. Therefore, if you assign the user a partition containing no agents, the standard real-time displays contain no agent data. In this case, the user must create a private display and apply a filter or the supervisor/reporting agent combination to see agent data. For more information, see “Partitions and supervisor/reporting agent combinations in Real-Time Reporting” on page 470.

User types

To fully understand this feature, it is important to outline the difference between the Symposium Call Center Server user and the Web Client user.

User type	User definition	Created in
Symposium Call Center Server user	agents, supervisors, supervisor/agents	Contact Center Management or Configuration
Web Client user	Anyone who logs on to the application server and monitors the performance and activities of Symposium Call Center Server using Symposium Web Client. This user can be a supervisor or an administrator.	Access and Partition Management → Users

After you create a supervisor’s Symposium Call Center Server user profile in Contact Center Management (or Configuration), to enable the supervisor to log on to the application server and use Symposium Web Client, you must also configure a Web Client user profile for this supervisor.

Note: Supervisors who do not need to use Symposium Web Client do not need a Web Client user profile; these supervisors only require a Symposium Call Center Server user profile.

When you configure the supervisor's Web Client user profile, you can create a link between two user profiles (the Web Client user profile and the supervisor's Symposium Call Center Server user profile) by using the **Supervisors** tab in Access and Partition Management. Each name on the **Supervisors** tab represents a supervisor *and* all his or her reporting agents on a per server basis. Therefore, when you link a supervisor's name with a Web Client user, you automatically enable this user to see *all* the supervisor's reporting agents.

This association is dynamic, meaning that each time a new agent is assigned to the supervisor, the agent is automatically associated with the supervisor's Web Client user profile (unlike agent partitions, which must be updated manually whenever a new agent is assigned to the supervisor). For more information, see "Agent partitions and supervisor/reporting agent combinations" on page 448.

You can use this feature to enable a supervisor to view all his or her *own* reporting agents, or you can enable one supervisor to see all the reporting agents of another supervisor. For more information, see "Supervisors and associated supervisors" on page 467. The following example shows how to enable supervisor Andrew Engel to view all his *own* reporting agents.

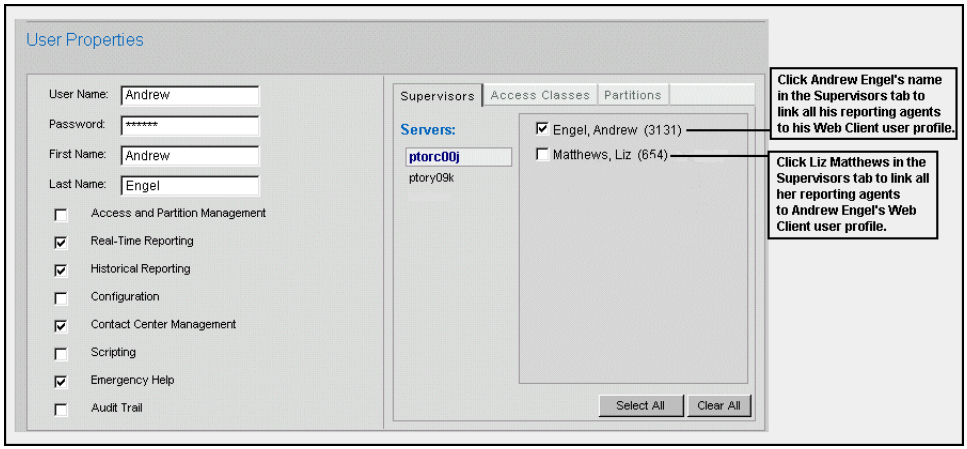
Example

In Contact Center Management you have created Symposium Call Center Server user profiles for supervisor Andrew Engel and the following five agents who report to him:

- Maggie Mok
- Sonia Braga
- George Smitts
- Jane Michkam
- John Nelson

The following graphic shows how you configure Andrew Engel's Web Client user profile in Access and Partition Management. This example assumes that you have assigned Andrew a partition in the Partitions tab. Then, click the check box beside Andrew Engel's name in the **Supervisors** tab to link both of his user profiles and enable him to see all his reporting agents in Real-Time and Historical Reporting and Contact Center Management (the components to which you have given him basic access).

Note: For more information about the effect of supervisor/reporting agent combinations in Real-Time Reporting, see “Partitions and supervisor/reporting agent combinations in Real-Time Reporting” on page 470. For a detailed listing of how this feature works in conjunction with partitions in each of the Symposium Web Client components (Real-Time and Historical Reporting and Contact Center Management), see Appendix E, “Supervisor/reporting agents matrix.”



Note: To enable Andrew Engel to see all the reporting agents of the other supervisor configured on server ptorc00j, click the check box beside Liz Matthews’ name. This way, Andrew Engel can act as the associated supervisor for her agents. For more information, see “Supervisors and associated supervisors” on page 467.

Supervisors and associated supervisors

You assign agents directly to a supervisor who has the primary responsibility for them. In the Symposium Call Center Server client, when this *primary* supervisor is unavailable, an *associated* supervisor provides backup by monitoring the agents in the real-time displays and historical reports.

In Symposium Web Client, the concept of an associated supervisor differs slightly from the Symposium Call Center Server client. Instead of designating associated supervisors, you can use two features—partitions or the supervisor/reporting agents feature—to share supervisors’ agents with other supervisors who can monitor their agents in their absence.

Note: In most cases, the supervisor/reporting agent feature only works in conjunction with a partition. If you do not assign a partition to the user, but only a supervisor/reporting agent combination, then the user sees all agent data. Private agent real-time displays and agent map displays are the exception to this rule. For details, see Appendix E, "Supervisor/reporting agents matrix."

While partitions enable you to assign *specific* agents to a Web Client user on a per server basis, the supervisor/reporting agents feature enables you to assign *all* of a supervisor's reporting agents to Web Client user on a per server basis. Partitions are useful, therefore, for assigning associated agents (*some* of a supervisor's agents to another supervisor), while the supervisor/reporting agents feature is useful for assigning *all* of a supervisor's reporting agents. You can use partitions alone, or a combination of both features, to control the agent data that Web Client users can see.

Example

The company Best Air has two sales departments, Europe and Canada. The two corresponding supervisors for each department are Andrew Engel and Liz Matthews. The administrator creates two partitions for the call center, one for each supervisor. Each partition contains all the *associated* agents for each supervisor, plus the required skillsets, CDNs, DNIS, applications, and report groups. The administrator also assigns a supervisor/reporting agent combination to each supervisor, enabling them to automatically view all their own *reporting* agents.

In this example, supervisor Andrew Engel has five agents reporting directly to him. These agents are assigned to him in Contact Center Management, and are assigned to his Web Client user profile through the supervisor/reporting agents feature in Access and Partition Management. The partition assigned to him includes seven of the ten agents who report directly to Liz Matthews, making Andrew the associated supervisor for these seven agents. When Liz is unavailable, Andrew can monitor these seven agents in the real-time displays, historical reports, and Contact Center Management, in addition to his own reporting agents.

Result in Real-Time Reporting

In Real-Time Reporting, Andrew can create and use filters to specify the partitioned agents he wants to see in the private agent real-time displays—in this case, Liz's agents (Andrew's associated agents). He can also assign his supervisor/reporting agent combination to these real-time displays so he can see

his reporting agents. He can assign only a filter, only the supervisor/reporting agent combination, or both (if he wants to see all 12 agents in the display). For more information, see “Partitions and supervisor/reporting agent combinations in Real-Time Reporting” on page 470.

Result in Historical Reporting

In Historical Reporting, Andrew can use the selection criteria to specify the agents he wants to include in reports.

Result in Contact Center Management

Andrew sees all the agents included in the partition assigned to him (his associated agents) and the agents included in the supervisor/reporting agent combination assigned to him (his reporting agents) in the windows to which he has been given access. For more information, see “Partitions and supervisor/reporting agent combinations in Contact Center Management” on page 473.

Note: To make Andrew Engel the associated supervisor for *all* of Liz’s reporting agents, instead of manually adding all the agents to a partition and assigning the partition to Andrew, use the supervisor/reporting agents feature to link Liz Matthews’ profile with Andrew’s Web Client user profile. For more information, see “Agent partitions and supervisor/reporting agent combinations” on page 448.

Partitions and supervisor/reporting agent combinations in Symposium Web Client components

When you assign partitions and supervisor/reporting agent combinations to a Web Client user, the agent data appears in different ways in Real-Time Reporting, Historical Reporting, and Contact Center Management.

Note: For a detailed listing of how the supervisor/reporting agents feature works in conjunction with partitions in each of the Symposium Web Client components (Real-Time and Historical Reporting and Contact Center Management), see Appendix E, “Supervisor/reporting agents matrix.”

Partitions and supervisor/reporting agent combinations in Real-Time Reporting

Partitions and the supervisor/reporting agents feature behave differently in Real-Time Reporting, based on the type of display the user opens, and whether the user assigns a supervisor/reporting agent combination or a filter to the display (or, in some cases, both). For a complete listing of how partitions and supervisor/reporting agent combinations affect each type of display, see Appendix E, "Supervisor/reporting agents matrix."

Filters

When you assign a Real-Time Reporting user a partition, the user can decide which data he or she wants to see by creating a filter containing the desired data and assigning the filter to the private real-time displays.

Supervisor/reporting agent combinations

Just as the user can assign a filter to a private display so that he or she sees only the filtered information in the display, so too can the user assign a supervisor/reporting agent combination to view all the applicable reporting agents in the agent display. Both the filters the user has created and the supervisor/reporting agent combinations assigned to the user appear on the **Filters** tab in Real-Time Reporting. The user can assign a filter, a supervisor/reporting agent combination, or sometimes both, to a display. For more information on Real-Time Reporting, see Chapter 3 in the *Symposium Call Center Web Client Supervisor's Reference Guide*.

This section outlines the differences in the following three types of displays:

- **standard real-time displays** Since users cannot apply either filters or supervisor/reporting agent combinations to standard displays, only partitioned data is shown in this type of display. If you do not assign a partition to a user, therefore, the user sees all data in the standard displays. If the partition contains no agents, then the user sees no agent data in the display, regardless of whether you have assigned a supervisor/reporting agent combination to the user.
- **private agent real-time displays** If you assign the user a partition, then the user can choose the data he or she wants to see in the display by creating a custom filter and assigning it to the display. If you assign the user a supervisor/reporting agent combination (in Access and Partition Management), the user can also assign the combination to the display to

view the corresponding reporting agents. The user can assign a filter, a supervisor/reporting agent combination, or both, to the display.

- **agent map graphical displays** Agent map graphical displays are similar to private agent real-time displays, except users *must* assign either a filter or a supervisor/reporting agent combination to the display, but cannot assign both at the same time.

The following table summarizes all scenarios and the results in Real-Time Reporting. Since supervisor/reporting agent combinations are applicable only to private agent real-time displays and to agent map graphical displays, this example focuses on these two types of displays.

In this example, it is assumed that you have assigned the user a partition containing agents and the supervisor/reporting agent combination containing all the user's reporting agents. For a more detailed look at the results of supervisor/reporting agents combinations and partitions in Real-Time Reporting, see Appendix E, "Supervisor/reporting agents matrix."

Type of display	User assigns this to the display	What the user sees in the display
Standard real-time display	Users cannot assign filters or supervisor/reporting agent combinations to standard displays.	Only the agents (and any other data) included in the partitions assigned to the user. Supervisor/reporting agent combinations are not applicable to standard real-time displays and, therefore, the agents included in these combinations do not appear.
Private agent real-time display	The user does not assign anything to the display (neither a filter containing partitioned agents, nor a supervisor/reporting agent combination).	All the agents in the user's partition. The agents in the supervisor/reporting agent combination do not appear.

Type of display	User assigns this to the display	What the user sees in the display
Private agent real-time display	The user assigns a filter containing a subset of their partitioned agents, but does not assign a supervisor/ reporting agent combination.	Only the partitioned agents that the user has added to the filter, not the reporting agents from the supervisor/ reporting agent combination.
	The user assigns a supervisor/reporting agent combination, but does not assign a filter containing partitioned agents.	Only the user's reporting agents.
	The user assigns *both* a supervisor/reporting agent combination, and a filter containing partitioned agents.	All the user's reporting agents, plus any partitioned agents that the user has added to the filter.
Agent map graphical display*	The user assigns a filter containing some of his or her partitioned agents.	Only the agents included in the filter, none of the agents in the supervisor/reporting agent combination.
	The user assigns a supervisor/reporting agent combination.	Only the user's reporting agents, none of the agents in the partition assigned to the user.

*The user must assign *either* a filter containing some of his or her partitioned agents or a supervisor/reporting agent combination to an agent map graphical display; the user must assign one of these to launch the display, but cannot assign both at the same time.

Partitions and supervisor/reporting agent combinations in Historical Reporting

In Historical Reporting, the **Selection Criteria** box contains all data included in the partitions and supervisor/reporting agent combinations assigned to the user. If you do not assign the user a partition, then the user sees *all* agent data in this box, regardless of whether you have assigned the user a supervisor/reporting agent combination.

The agents in the supervisor/reporting agent combinations assigned to the user appear individually in the **Selection Criteria** box, and are not grouped under the supervisor's name (as on the Filters tab in Real-Time Reporting). Each type of data is included in a filter (for example, an Agent Name filter, or an Agent Login ID filter). The available filters depend on the type of statistics included in the report. For example, the Agent Performance report may contain two filters—Agent Name and Agent Login ID. When the user selects either filter, then all agents included in the partitions and supervisor/reporting agent combinations assigned to the user (on the selected server) appear in the **Selection Criteria** box. For more information on Historical Reporting, see Chapter 4 in the *Symposium Call Center Web Client Supervisor's Reference Guide*.

For a more detailed look at the results of supervisor/reporting agents combinations and partitions in Historical Reporting, see Appendix E, "Supervisor/reporting agents matrix."

Partitions and supervisor/reporting agent combinations in Contact Center Management

Normally, users whose access class enables them to work only with assignments are supervisors. These users can only create ad hoc agent to supervisor and agent to skillset assignments; they cannot add, edit, create, or delete users, or schedule assignments. Users who can perform all functions in Contact Center Management have administrator privileges in this component.

Users with administrator privileges usually need to see *all* supervisors and agents in Contact Center Management so they can perform their required duties, such as editing and deleting user profiles, and creating and scheduling assignments. The best way to ensure that these users always see all agents is to *not* assign a partition to them.

Note: If you only assign the user a supervisor/reporting agent combination and not a partition, then the user still sees all agents. Once you assign the user a partition containing agents, or a partition and a supervisor/reporting agent combination, then the user sees *only* the agents assigned to him or her.

Contact Center Management differs from Real-Time and Historical Reporting in that users require access class privileges to use this component. Not only can the access class restrict the actions the user can perform, but if you assign a user an access class containing the *Use Agent & Skillset Partitions in CCM* access level, then you restrict this user to seeing only their partitioned skillsets in Contact Center Management (in addition to their partitioned agents). If you do not assign this access level, then users can see all configured skillsets in the windows to which they have access in Contact Center Management.

Since most supervisors are restricted to viewing specific data in the call center, Symposium Web Client administrators usually assign partitions containing this data to them. As an added way of controlling the data that supervisors can see, administrators can also assign supervisor/reporting agent combinations to them.

The following table summarizes the effect that agent and skillset partitions and supervisor/reporting agent combinations have on Contact Center Management. For a more detailed look at the results of supervisor/reporting agent combinations and partitions in Contact Center Management, see Appendix E, “Supervisor/reporting agents matrix.”

IF	THEN the user sees
you do not assign the user a partition or a supervisor/reporting agent combination	everything, all agent and skillset data regardless of whether you assign the *Use Agent & Skillset Partitions in CCM* access level or not
you assign the user a partition containing no agents, and do not assign a supervisor/reporting agent combination	no agent data
you do not assign the user a partition, but you assign the user a supervisor/ reporting agent combination	all agent data

IF	THEN the user sees
you assign the user a partition containing no agents, and a supervisor/ reporting agent combination	only the agents in the supervisor/ reporting agent combination
you assign a partition containing agents, but no skillsets, and you assign the *Use Agent & Skillset Partitions in CCM* access level	no skillsets, just the agents included in the partition
you assign a partition containing skillsets, but no agents, and no supervisor/reporting agent combination, and you assign the *Use Agent & Skillset Partitions in CCM* access level	the skillsets in the partition, but no agent data (the user cannot work with agents)
you assign a partition containing skillsets, but no agents, and a supervisor/reporting agent combination, and you assign the *Use Agent & Skillset Partitions in CCM* access level	the skillsets in the partition, and the agents in the supervisor/reporting agent combination
you assign the user a partition containing agents and a supervisor/ reporting agent combination	the agents included in the partition *and* the agents in the supervisor/reporting agent combination

Sample task flow for configuring Web Client users

In this example, your call center contains three supervisors on the Toronto server: John, Sheila, and Cathy. Each supervisor has 10 reporting agents. You assign a combination of partitions and supervisor/reporting agents to arrange the following scenario:

- Each supervisor can automatically see all 10 of their reporting agents in the real-time displays, historical reports, and in Contact Center Management (assuming they have access to these components).

- In addition to his own 10 agents, John can see 5 of Cathy's agents so he can manage them when she is on break.
- In addition to her own 10 agents, Sheila can see the remaining 5 of Cathy's agents so she can manage them when Cathy is on break.

The following table summarizes this scenario:

Supervisor	Agents the supervisor can see in Symposium Web Client
John	■ his 10 reporting agents ■ 5 of Cathy's agents
Sheila	■ her 10 reporting agents ■ the other 5 of Cathy's agents
Cathy	■ her 10 reporting agents

High-level task flow

The following table gives a high-level overview of the steps you need to perform to arrange the scenario listed in this example. For detailed procedures, see the online Help included with the application.

Perform this step	in this component
1 Create the Symposium Call Center Server user profiles for the 3 supervisors, John, Cathy, and Sheila.	Contact Center Management
2 Create the Symposium Call Center Server user profiles for the 30 agents, assigning the appropriate 10 agents to each of the 3 supervisors created in step 1.	Contact Center Management
3 Create any custom report groups that the supervisors require to share customized report templates. **Note:** If the supervisors do not need to share customized reports, then you do not have to create report groups.	Access and Partition Management → Report Groups

Perform this step	in this component
4 Only if the supervisors need to work in Contact Center Management, create the access classes that they will need to perform their duties in this component. **Note:** Access classes are only required to work in Configuration, Scripting, and Contact Center Management. If the supervisors require access to Contact Center Management, then you must create an access class including *CCM* access, *Agent to Supervisor Assignment* access or *Skillset Assignment* access on at least one server. You can also ensure that users only see their partitioned skillsets in Contact Center Management by using the *Use Agent & Skillset Partitions in CCM* access level. If you do not use this access level, then users automatically see all configured skillsets in Contact Center Management. To enable the supervisors to work only with ad hoc assignments in this component, then assign the *Ad Hoc Assignments* access level for the appropriate type of assignment; the *Schedule Assignments* access level gives the user access to the assignments view where users can save and schedule assignments.	Access and Partition Management → Access Classes

Perform this step	in this component
5 Create partitions for the supervisors, specifying the agents, applications, skillsets, CDNs, DNISs, and report groups that belong in each partition. For this example, create ■ partition A, containing the 5 agents of Cathy's that John will monitor in her absence (along with all the required skillsets, and any applications, CDNs, DNISs and report groups that John needs to view) ■ partition B, containing the remaining 5 agents of Cathy's that Sheila will monitor in Cathy's absence (along with all the required skillsets, and any applications, CDNs, DNISs and report groups that Sheila needs to view) ■ partition C, containing the applications, CDNs, DNISs, and report groups that Cathy needs to view	Access and Partition Management → Partitions
6 Create the Web Client user profiles for each of the three supervisors.	Access and Partition Management → Users
7 Assign each Web Client user basic access rights to the components they need to use. **Note:** Typical supervisors require basic access to Real-Time and Historical Reporting, Contact Center Management, and Emergency Help.	Access and Partition Management

Perform this step	in this component
8 Assign each Web Client user the appropriate supervisor/reporting agent combination, enabling the user to automatically see all their reporting agents. For more information, see the "Supervisor/reporting agents feature" on page 464. **Note:** In this example, you assign John's supervisor profile (and all his reporting agents) to John's Web Client user profile. Perform the same procedure for both Sheila and Cathy.	Access and Partition Management → Users → Supervisors tab
9 Assign each Web Client user the appropriate access class.	Access and Partition Management → Users → Access Classes tab
10 Assign each Web Client user the appropriate partition. In this example, you assign to John's Web Client user profile partition A, containing the 5 agents of Cathy's that he needs to monitor in her absence (along with the appropriate skillsets, applications, CDNs, DNISs, and report groups). You assign partition B to Sheila and partition C to Cathy. **Note:** If you assign Cathy new agents that you want John or Sheila to monitor in Cathy's absence, then you must update the partitions assigned to John and Sheila to include the new agents. Alternately, to enable John or Sheila to automatically view *all* Cathy's agents, assign Cathy's supervisor profile (and all her reporting agents) to John's and Sheila's Web Client user profiles.	Access and Partition Management → Users → Partitions tab

Perform this step	in this component
11 Click **Submit** after configuring each user profile. **Result**: When John, Sheila, and Cathy open Symposium Web Client, they can ■ log on and use the components to which you have given them basic access ■ perform the functions their access class enables them to do in Contact Center Management (assuming they have basic access to this component) ■ see all their own reporting agents ■ see the additional agents and the data included in the partitions assigned to them	Access and Partition Management

Section E: Audit Trail

In this section

Overview 482
Monitored resources 484

Overview

Introduction

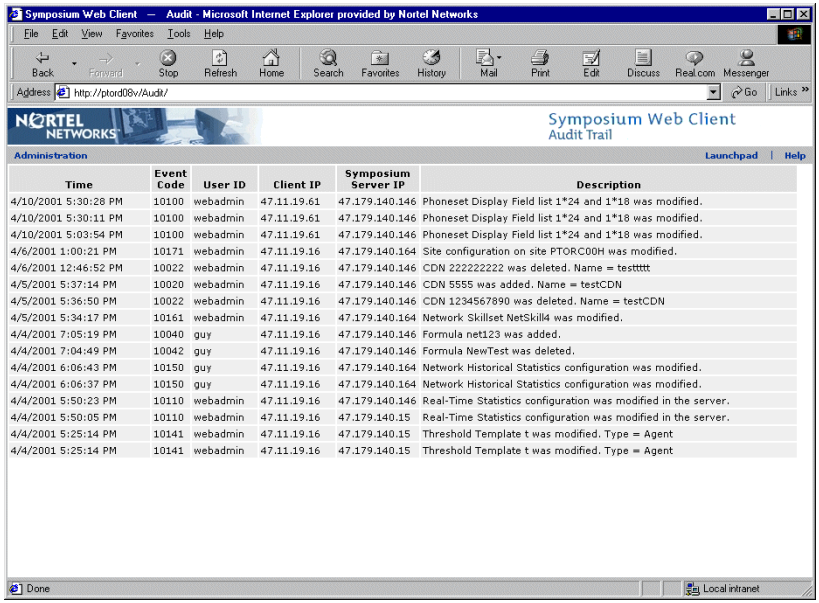
Audit Trail allows you to view the most recent actions that users have performed in Symposium Web Client's Configuration component and in the automated assignments feature of Contact Center Management. You can view these changes in a log, and identify which user made the changes.

Note: Audit Trail does not track any changes made on the Symposium Call Center Server client.

Accessing Audit Trail

You can access Audit Trail by clicking Audit Trail on the Symposium Web Client launchpad.

Audit Trail Log window



You can configure the total number of events that Audit Trail stores by clicking Administration on the toolbar. You can store up to 10 000 events in the database; however, the more events you choose to store, the longer the system takes to retrieve the event information and display it online.

Monitored resources

Audit Trail monitors any additions, modifications, or deletions that a user makes to the following resources:

- call presentation classes
- formulas
- activity codes
- CDNs
- DNISs
- IVR ACD-DNs
- phonesets and voice ports
- route numbers
- skillsets
- threshold templates

Audit Trail also monitors any modifications that a user makes to the following resources:

- network historical statistics configuration
- global settings
- historical statistics configuration
- networking communication parameters
- real-time statistics configuration

Audit Trail also monitors whether agent to skillset and agent to supervisor assignments were created successfully using the automated assignments feature. For one of these assignments to be successful, you must create an XML file that meets specific criteria and the file must be parsed by the automated assignments utility on the application server. Audit Trail records both successful and failed assignments. For more information on this feature, see “Using the XML automated assignments feature” on page 426.

Note: Audit Trail does not record changes made using Symposium Call Center Server client PCs, nor does it record the success or failure of assignments created in the Contact Center Management component.

Section F: Scripting

In this section

Overview	488
Viewing scripts	489
Creating and editing scripts	490
Validating your script	492
Displaying script variables and parameters	493
Viewing, editing, and assigning application threshold classes	495
Working with sample scripts	497
Checking variables for referencing scripts	499

Overview

Introduction

The Scripting component of Symposium Web Client enables you to write scripts that determine the sequence of steps a call follows once it enters the system. These steps can include call treatment, such as music or ringback, skill-based routing, and IVR.

While working in the Scripting component, you can perform the following procedures (provided that a user with administrator privileges has given you the appropriate access privileges):

- View existing scripts.
- Create and edit scripts.
- Validate scripts.
- Display all script variables and corresponding parameters.
- View, edit, and assign application threshold classes.

Note: If you need to perform one of the above actions, but cannot access the necessary Scripting component, request that your administrator review your access class privileges. He or she may need to update your Scripting access privileges. For more information on Scripting access classes, see the online Help.

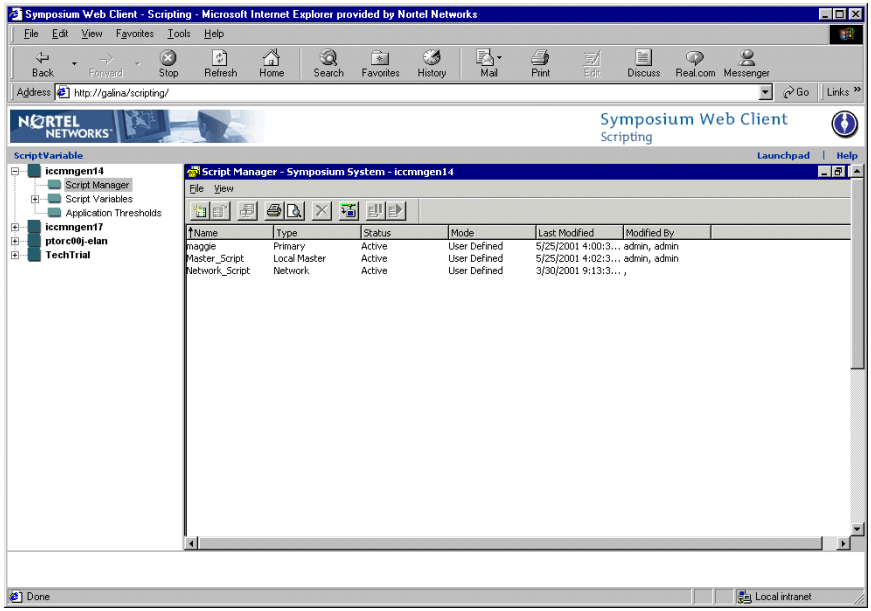
This section provides you with a high-level overview of the Scripting component. For detailed step-by-step procedures, see the online Help in the Symposium Web Client application.

Viewing scripts

Introduction

You can view a list of the existing scripts for a specific server in Symposium Call Center Server. On the system tree, double-click the server in Symposium Call Center Server to expand the tree, and then click **Script Manager**.

Script Manager window



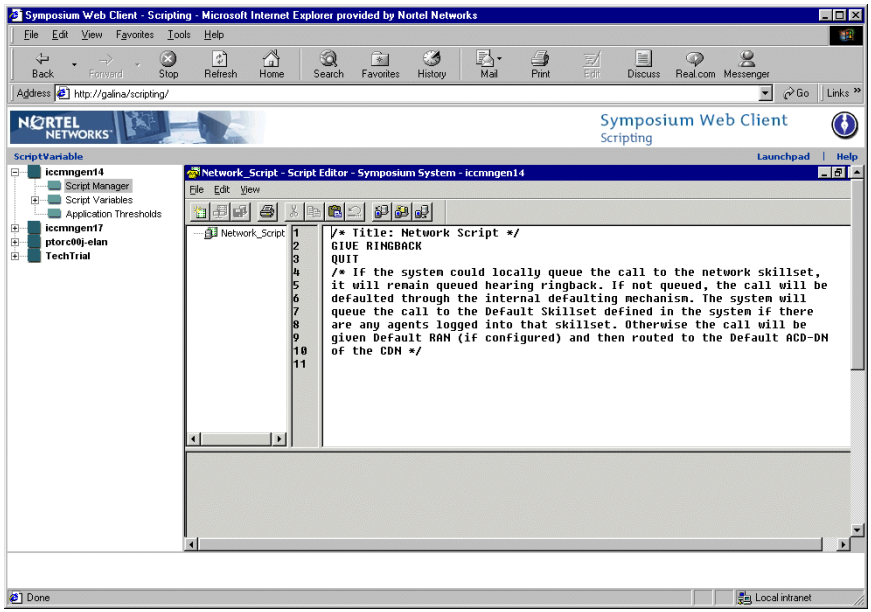
You can display and edit any of the scripts in this window by double-clicking the script that you want to see. The script opens in the Script Editor window where you can modify the call routing instructions.

Creating and editing scripts

Introduction

In the Script Manager window, you can click **File → New** to create a new script, or double-click an existing script to edit it in the Script Editor window. You can make changes to activated scripts, and to scripts that are validated but not activated.

Script Editor window



Note: While writing or editing a script in the Script Manager window, you can click **View → Script Commands** to launch the Script Command Reference window, which allows you to insert script elements, such as commands, operators, events, intrinsics, and variables.

Once you make your changes to a script, click **File → Save** to save a validated (inactive) script and **File → Activate** to save and activate your changes to an active script. If you are saving a new script, click **File → Save**, and assign a unique name to your script that does not exceed 30 000 characters.

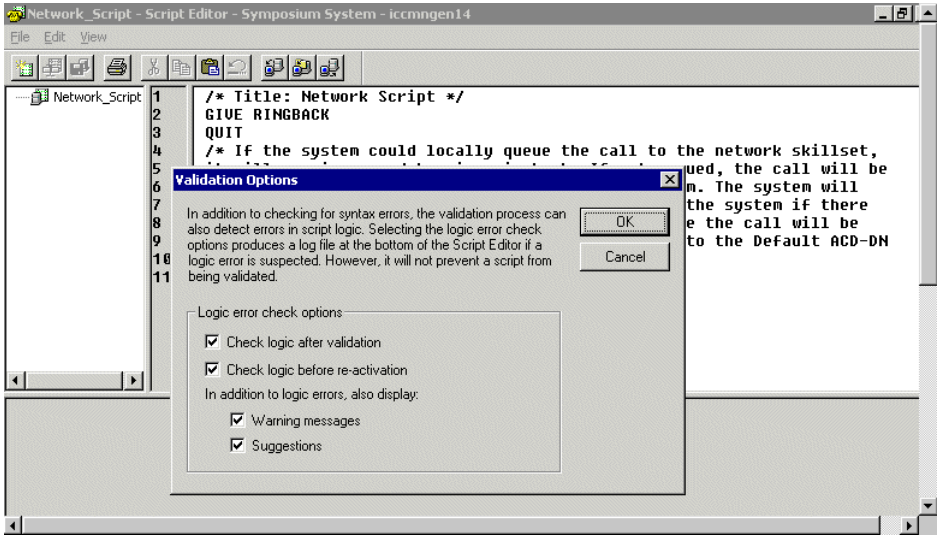
Validating your script

Introduction

You can set the validation options so that the application informs you when you are breaking scriptwriting rules. The rules are designed to eliminate run-time errors that result in improper routing of calls in Symposium Call Center Server.

In the Script Editor window, click **View → Validation Options** to display the Validation Options window.

Validation Options window



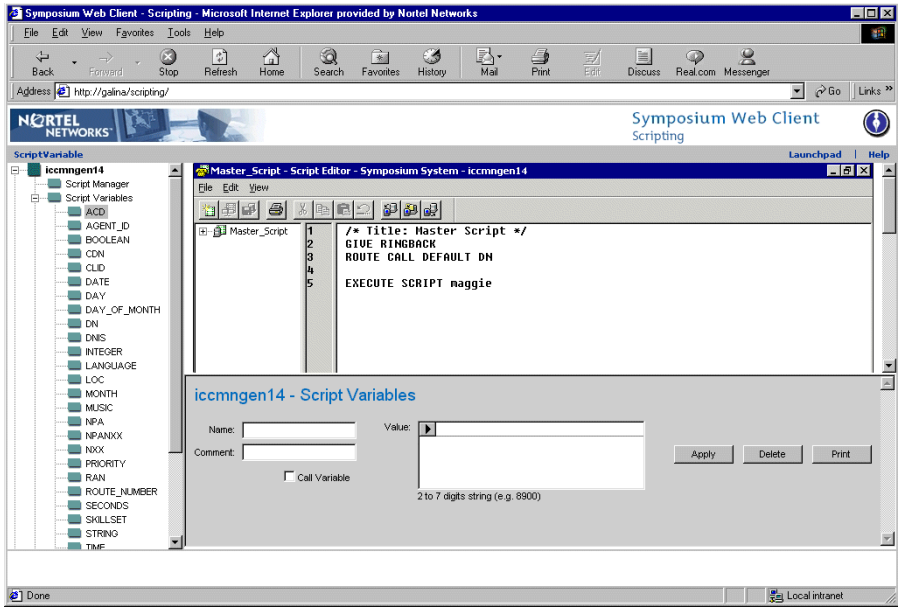
You can configure validation options to enforce scriptwriting rules automatically after a script has been successfully validated, or before an activated script is edited and then reactivated. You can also configure validation options to display warning messages.

Displaying script variables and parameters

Introduction

When you click **Script Variables** on the system tree, the Script Variables tree appears, displaying all variables configured on the server. To view a specific script variable, click the variable on the tree. The variable appears in the Script Variables window. The parameters of the variable appear in the boxes at the bottom of the window.

Script Variables window



Script variables, like variables used in any programming language, represent a value. You can define a script variable in the Script Variables window and use it in more than one script. When you change a variable in the Script Variables window, all occurrences of that variable are also changed.

Before you create script variables, all system resources, such as RAN routes, music routes, voice ports, CDNs, IVR-DNs, and call treatments must be set up. In addition, all skillsets and agents must be configured on the selected server. And finally, if you plan to create voice segment variables, all of the voice segments must be created.

Viewing, editing, and assigning application threshold classes

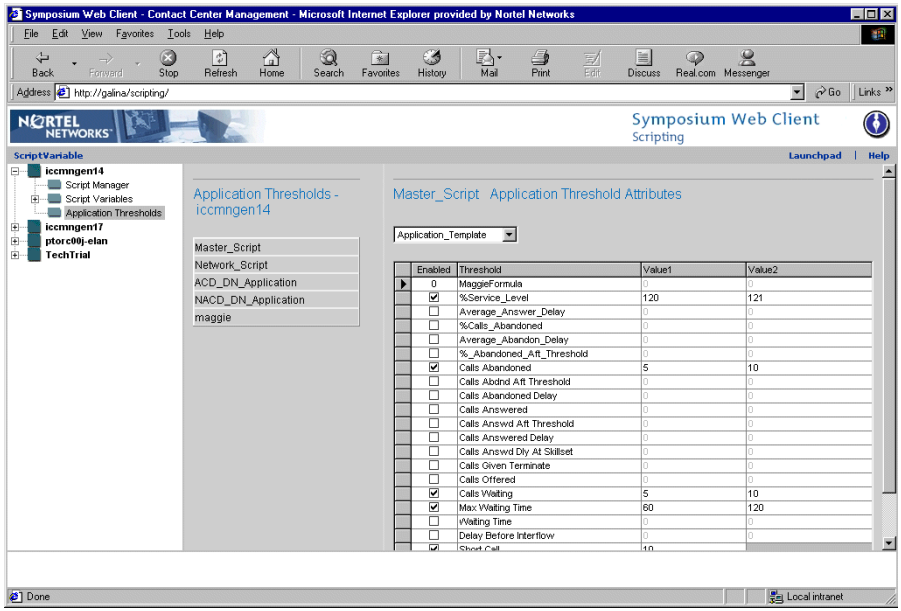
Introduction

You can view and edit threshold classes, and assign them to applications in the Scripting component. However, to create new threshold classes or to delete threshold classes, you must use the Threshold Classes window in the Configuration component.

Applications are used for reporting purposes. For the master script and each activated primary script called by the master script, the system automatically creates an application with the same name as the script.

Note: There are no scripts associated with the ACD_DN application or the NACD_DN application.

Application Thresholds window



To view, edit, or assign application thresholds, click the **Application Thresholds** icon under the appropriate server on the system tree. From the list of applications in the left pane of the window, select the application for which you want to view thresholds. In the right pane, from the drop-down list, select the threshold class. You can make the changes in the table that appears below the drop-down list.

Note: For the new threshold values to take effect, you must click the **Enabled** check box beside the application threshold.

Applications track information about calls, call types, and conditions in the call center. Call center managers and supervisors can view this information by using real-time displays or by running reports against the applications. You can assign thresholds to applications by creating application threshold classes in the Threshold Classes window of the Configuration component, and then applying that threshold class to the application. For a complete list of application thresholds, see the *Symposium Call Center Server Administrator's Guide*.

Working with sample scripts

Introduction

When you install Symposium Web Client on the application server, it automatically installs sample scripts in the following default location:

c:\Program Files\Nortel Networks\WClient\Server

where *c*: is the drive on which you installed Symposium Web Client.

To use these sample scripts, you must perform the following procedure:

- Import the sample scripts that you want to use from the application server into Symposium Web Client by using the Import command in the Scripting component. The Import command adds the text of the imported script to any text in the current script.

ATTENTION

For detailed information on sample scripts, see the *Nortel Networks Symposium Call Center Server Scripting Guide*.

Note: The variables used in the sample scripts are examples only. If you use a sample script that contains variables, you must create and define the variables on your system.

Before you begin using sample scripts, verify the following:

- All system resources, such as RAN routes, music routes, voice ports, call treatments, DNs, and IVR DNs are set up.
- All variables, agents, and skillsets are created.
- All voice segments for voice prompts are created.

To import sample scripts into Symposium Web Client

To use the sample scripts in Symposium Web Client, you can import them into either an existing script or a new script in the Scripting component. The Import command adds the text of the imported sample script at the end of any text in the current script.

1 You can import a sample script in Symposium Web Client into two different types of scripts:

   a. To import a sample script into an *existing* script, in the Script Manager, double-click the script into which you want to import the sample script.

   Result: The script opens in the Script Editor.

   b. To import a sample script into a *new, blank* script, in the Script Manager, click File → New.

   Result: The Script Editor opens with a blank starting page.

2 In the Script Editor, click File → Import.

   Result: The Open dialog box appears.

3 From the **Look in** drop-down list, navigate to the sample scripts on the application server. The default location is *c*:\Program Files\Nortel Networks\WClient\Server, where *c*: is the drive on which you installed Symposium Web Client.

4 Select the sample script that you want to import.

5 Click **Open**.

   Result: The system adds the text of the sample script to the end of the current script.

ATTENTION

The script that you import may contain references to variables. Variables are not imported with the script. You must define the variables on your system.

Checking variables for referencing scripts

Introduction

You can use this procedure to check whether a variable is referenced by any active scripts. If a script variable is referenced by any active scripts, you cannot change its properties (except for its value), rename it, or delete it.

To check variables for referencing scripts

On the system tree, right-click the variable that you want to check.

Result: If the variable is referenced in any activated scripts, then the system lists the script names in a pop-up box. If the box does not appear, then the variable is not referenced in any activated scripts.

Chapter 7

Troubleshooting

In this chapter

Technical support 502

Client PC 507

Application server 517

Simple Object Access Protocol errors 531

Technical support

Introduction

If you experience technical difficulties, ensure that you have downloaded the latest Service Updates, Performance Enhancement Packages (PEPs), and addenda for both Symposium Call Center Server and Symposium Call Center Web Client. You can download the latest installation or documentation addendum from either http://www.nortelnetworks.com (for end customers), or http://www.nortelnetworks.com/prd/picinfo/ (for distributors), and the latest Service Updates and PEPs from https://www21.nortelnetworks.com/MPL (for Europe), or from https://www43.nortelnetworks.com/MPL (for North America).

Note: To register for either of these MPL web sites, follow the instructions listed at http://nortelnetworks.com/register.

Nortel Networks personnel use pcAnywhere as a remote support tool. If you require remote support from Nortel Networks, you must install and configure pcAnywhere Version 10.5 on the application server.

Note: If you have a previous version of pcAnywhere installed on the application server, consult the Symantec web site (www.symantec.com/pcanywhere) to find out whether you must uninstall your version before installing pcAnywhere 10.5.

Installing and configuring pcAnywhere 10.5 for Symposium Web Client

When you install pcAnywhere 10.5, the installation program offers you a choice between a standard or an advanced software package. To be compatible with Symposium Web Client, choose the standard software package. Use the Windows 2000 Add/Remove Programs utility in the Control Panel to install the software.

Note: If the installation wizard asks if you want to preserve configuration data from a previous version after the uninstall, select **No**. Configuration data from previous versions of pcAnywhere is incompatible with pcAnywhere version 10.5.

ATTENTION

Do not follow the installation and configuration procedures in the Symposium Call Center Server documentation. These procedures do not apply to Symposium Web Client because Remote Access Service (RAS) is not used.

CAUTION

Risk of system failure

Before you install pcAnywhere version 10.5, ensure that the video drivers on the application server PC are current by consulting the driver manufacturers' Web sites for any available updates. Failure to do so can result in the appearance of a blue screen after pcAnywhere installation or after use of pcAnywhere for operations such as file transfer. For more information, refer to the pcAnywhere web site at www.symantec.com/pcanywhere.

To install pcAnywhere 10.5

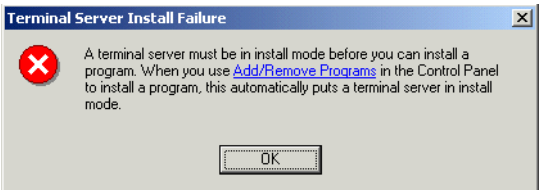
The following steps are general guidelines only. For more complete information, see the documentation included with the pcAnywhere software.

1 Log on to the application server as **Administrator**.

2 Insert the pcAnywhere Version 10.5 CD into the server.

3 If autorun starts and you click **Install**, or if you clicked the setup.exe file on the CD, the Terminal Server Install Failure dialog box appears. This occurs

because Terminal Services must be in Install Mode before you can install an application.



4 Click **Add/Remove Programs** to open the Add/Remove Programs window.

5 Click **Add New Programs**.

6 Click **CD or Floppy**.

7 Click **Next**. The program finds the setup.exe file on the CD.

8 Click **Next**. The pcAnywhere 10.5 launchpad appears.

9 Click **Install pcAnywhere 10.5**.

10 For the standard installation, click **pcAnywhere for the Individual**.

11 Click **Next**.

12 Follow the prompts in the wizard to install pcAnywhere 10.5.

13 When the wizard prompts you to

- choose a setup type, choose **Typical**
- download and install updates, click **Next** to install all updates it finds
- register pcAnywhere, click **Skip**. Then click **Yes** when it asks you to confirm your choice.

14 Click **Finish** when the installation is complete.

15 When the wizard prompts you to restart the server, click **Yes** to restart.

To start pcAnywhere 10.5 for the first time

Tip: To ensure optimum speed when using pcAnywhere, before starting the program, configure the Active Desktop settings on the server as follows:

a. Right-click anywhere on the server desktop.

b. On the resulting pop-up menu, highlight **Active Desktop** until another pop-up menu appears.

c. On this pop-up menu, ensure that Show Web Content is not selected.

1 Log on to Windows as **Administrator**.

2 From the Windows Start menu, choose Programs → Symantec pcAnywhere.

Note: If the system asks you to register pcAnywhere, select **Skip**, and then choose **Yes** when asked to confirm.

ATTENTION

If the following message appears, it indicates that your video driver is incompatible with pcAnywhere: “pcAnywhere detected and fixed a display driver problem. Please restart your computer to allow the change to take effect.” In this case, you must uninstall pcAnywhere, update your video driver, and then reinstall pcAnywhere.

Result: The pcAnywhere Manager window appears.

3 Continue with the following procedure to configure pcAnywhere 10.5.

To configure pcAnywhere 10.5

Configuration of pcAnywhere sets up a secure caller account to access the server. You can add a caller account for each remote PC. These caller accounts restrict usage of pcAnywhere to appropriate users (for example Nortel Networks support personnel and distributors).

1 In the pcAnywhere Manager window, ensure the **Hosts** button is selected.

2 Right-click the **Network, Cable, DSL** icon and select **Properties**.

Result: The pcAnywhere Host Properties: Network, Cable, DSL window appears.

3 Ensure that the check box beside TCP/IP is checked.

4 Click the **Settings** tab.

5 Ensure that **Launch with Windows** and **Run Minimized** are checked and leave all other default settings.

6 Click **Apply** to save your settings.

7 Click the **Callers** tab.

8 From the Authentication Type drop-down list, select **pcAnywhere**.

9 Below the Caller list heading, click the **New item** icon.

Result: The pcAnywhere Caller Properties: New Caller window appears.

10 On the Identification tab, in the **Login Name** box, type a name for the caller account. You can choose any name, or use a name that is familiar to you, such as NGenDist.

11 In the **Password** box, type the password for the caller account.

Tip: If you typed NGenDist for the login name, you can use the same NGenDist password that is used in Symposium Call Center Server, or you can use a password of your choice.

12 In the **Confirm Password** box, type the same password again.

13 Click **Apply** to save your changes.

Result: The Callers tab reappears.

14 Click the **Privileges** tab.

15 Click the **Superuser** radio button.

16 Click **Apply**.

17 Click **OK** to return to the Callers tab.

18 Repeat steps 9 to 17 to create another caller account (for example, NGenDesign).

Tip: If you typed NGenDesign for the login name of the second caller account, then you can use the same NGenDesign password that is used in Symposium Call Center Server, or you can use a password of your choice.

19 Click the **Security Options** tab.

20 Under Login Options, ensure that **Limit login attempts per call** and **Limit time to complete login** are checked and set to **3**. Ensure that the Encryption Level is set to **none**, and the Session options are set to **Host and Remote**.

21 Click the **Conference** tab.

22 Ensure that **Enable conferencing** and **Obtain IP address automatically** are selected.

23 Click **Apply** to save your settings.

24 Click the **Protect Item** tab if you want to assign a password to control who can modify the Network icon settings. Otherwise, skip to step 25.

25 Click **OK** to save all pcAnywhere Host settings.

Client PC

Are you having problems with Internet Explorer?

Checklist

- Check that you are using the correct version of Internet Explorer on the client PC (version 5.5 with Service Pack 2 or later).
- Check that you have configured security in Internet Explorer correctly. For more information, see the “Installing and configuring the browser on a client workstation” on page 292.
- If you are getting error messages from Internet Explorer indicating that your web site cannot run Out of Process Components, follow these steps:

To enable Out of Process Components

1 Create a script called AspAllowOutOfProcComponents.vbs using any text editor. Insert the following commands:

```
Set objWebService = GetObject("IIS://LocalHost/w3svc")

' Enable AspAllowOutOfProcComponents.

objWebService.Put "AspAllowOutOfProcComponents", True

 ' Save the changed value to the metabase.

objWebService.SetInfo
```

2 Save the script.

3 In Windows Explorer, double-click the script.

4 If this fails, reinstall the software.

Are you having display problems?

If the layout of the web interface in Symposium Web Client is distorted, follow these steps.

To check the display settings of your computer

1 Click Start → Settings → Control Panel.

2 Double-click the **Display** Icon.

3 On the **Settings** tab, drag the slider in the **Desktop area** box until the value reads at least 1024 x 768 pixels (it cannot be lower than this value).

4 From the **Font size** drop-down list, select Small Fonts.

5 Click **OK** to save your changes.

To set the font size in Internet Explorer

In Internet Explorer, on the View menu, click Text Size → Medium.

To resize the font

If the text or content displayed in Internet Explorer is too large for the window, and you cannot resize the window, do the following:

In Internet Explorer, on the View menu, click Text Size → Smaller, or Text Size → Smallest.

Are you having problems logging on to the application server?

When you attempt to log on to the application server either as the default administrator, *webadmin*, or as another user, do you receive the following error message?

"*You have entered an invalid User name/password combination. If you have forgotten the password, please contact your administrator.*"

If you are receive this message, it may be because you changed the default password for the Windows 2000 Server user that is created during the installation of the Symposium Web Client software, *iceadmin*. If you changed the password for this user in Windows after you installed the software, then you cannot log on to the application server. In this case, you must uninstall and reinstall the Symposium Web Client software, ensuring that you do not alter the default user name and password for the *iceadmin* account.

Are you having problems with real-time displays?

Note: For more troubleshooting tips on real-time displays, including a description of the error messages that appear in unicast and multicast environments, see “Are the real-time displays blank?” on page 521.

You cannot launch real-time displays

In Symposium Web Client, for the real-time displays to launch properly, the system downloads and registers a new RTDControl to the client PC when you launch a real-time display for the first time. If you cannot launch real-time displays on a client PC, then it may be because you have enforced user policies that deny access to the registry on the PC, and, therefore, prevent the system from downloading and registering the new RTDControl.

To download the RTDControl

1. Log on to the client PC as the local administrator (or as a user with registry permissions).
2. Open Symposium Web Client.
3. Open the Real-Time Reporting component.
4. Launch a real-time display.

   Result: The system downloads and registers the required RTDControl to the client PC. Now regular users can log on to the client PC and launch real-time displays.
5. Perform this procedure on every client PC upon which real-time displays will be launched.

Note: If you are having problems downloading third-party controls to the client PC, it may be because of your local security settings. You must ensure that the local security settings for the policy *Unsigned non-driver installation behavior* are not set to *Do not allow installation*. For more information, see “To verify your local security policy settings” on page 310.

Copying and running the trace tool

You can use the IceRtdTrace tool to verify that client PCs are receiving multicast data from the application server. The IceRtdTrace tool resides on the application server. To use this tool on a client PC, you must copy the tool and its associated files to a removable media disk (for example, a CD), and then install them on the client PC.

To copy and run the trace tool

1 Navigate to the following path on the application server, where *x* is the drive on which Symposium Web Client is installed:

x:\Program Files\Nortel Networks\WClient\Server

2 Copy the following files to the removable media disk:

- ICERtdTrace.exe
- mtld.dll
- nbcfg95.dll
- nbcomd.dll
- nbdbapi.dll
- nbss95.dll
- nbss_e95.dll
- nicerr.dll
- ninccapi.dll
- nisysd.dll

3 Create a new folder, such as **Trace_Tools**, on the client PC that you are testing.

4 Copy the files from the removable media disk to the new folder on the client.

5 On the client PC, rename the file ICERtdTrace.exe to a new name that has a maximum of eight characters (for example, IceTrace).

ATTENTION

The trace tool must be run from the MS-DOS command prompt, and MS-DOS does not accept names with more than eight characters on some Windows operating systems.

6 From the MS-DOS command prompt, change the directory to the folder on the client PC to which the files were copied, for example:

c:\>cd **Trace_Tools**

7 To check if data is being received by the client PC, type the following command:

IceTrace -r IPSend *<IP Multicast send address>*

If the client PC is receiving statistics from the application server, the data appears on the monitor. To stop the information from scrolling, press Ctrl+c. You can view the log file that captures the information, IPSndLog.txt, in the same directory.

No names appear in real-time displays

If the following symptoms appear in your real-time displays, then there may be a problem with the network settings or the configuration of your DNS server, or there may be delays in the network causing timeouts:

- Agent names and answering skillset names appear as **UNKNOWN** in agent real-time displays.
- Route names appear as **UNKNOWN** in route real-time displays.
- IVR queue names appear as **UNKNOWN** in IVR real-time displays.
- Skillset and application names appear incorrectly in skillset and application real-time displays.

Ensure that the network is functioning correctly, the DNS has been configured correctly on the application server, and that the DNS is providing responses within a reasonable time (for example, less than 10 seconds).

Are you having problems with historical reports?

Problem description: You open a private agent report for which you had chosen and saved agent names from the selection criteria. However, upon opening the saved report, instead of seeing the agent names in the Selected box, you see agent login ID numbers.

Solution: When you first open a report, the selection criteria defaults to the agent login IDs. However, the agent names that you selected are still saved with the report. To view them, perform the following step:

With the report open in the Report Properties window, from the filter drop-down list in the selection criteria area, select Agent Name again.

Result: The agent names that you originally chose replace the corresponding agent login IDs in the Selected box.

Problem description: When you launch an ad hoc report, the report viewer is blank.

Solution: You must install the required third-party files on the client PC for the Crystal Reports viewer to function properly. For details, see “Downloading the Crystal Reports Viewer” on page 315.

Are you having problems communicating with the application server?

When Symposium Web Client is installed, it uses the default settings stored in IIS. Ensure that web users have permissions on all directories in the Symposium Web Client web site. If they do not have permissions, contact your site administrator for details on changing the settings in IIS.

The computer name of the application server must be registered on the DNS server for client PCs to access the server and use Symposium Web Client. If the computer name is not registered on your DNS server, then Symposium Web Client will not function properly. If you have not configured a DNS server, then you must add the computer name of the application server to the HOSTS or LMHOSTS table on *each* client PC that accesses Symposium Web Client. For more information, see “Did you configure a name resolution server?” on page 513.

To test communication from the client to the application server

If the client cannot connect to the application server, and you have already checked to make sure that the Web Client user name and password are valid, follow these steps:

1. Ping the Symposium Web Client application server.
2. Check the IP addresses for the application server(s) and the server(s) in Symposium Call Center Server.
3. Check your cabling.
4. Make sure the web site is active on the application server.
5. Make sure the computer name of the application server is registered on the DNS server.

Contact your system administrator if the web site is active, the IP addresses are valid, and you are unable to successfully ping the Symposium Web Client application server.

To check if Internet Explorer uses a Proxy Server

If the client cannot connect to the application server, check whether Internet Explorer uses a Proxy Server.

On the Internet Explorer menu bar, click Tools → Internet Options → Connections → Lan Settings.

If the **User Proxy Server** check box is selected, contact your Proxy Server Administrator to verify that there are no restrictions preventing you from accessing the Symposium Web Client application server.

Did you configure a name resolution server?

If you did not configure a name resolution server during the operating system installation, then the client PCs that connect to Symposium Web Client cannot find the application server. In this case, your next step is to manually update the HOSTS or LMHOSTS tables on *each* client PC.

When you use server names to connect to an application server in TCP/IP networks, the server name must be associated with an IP address. LMHOSTS and HOSTS are host tables that carry out this association, which is called name resolution.

- The HOSTS table resolves host names to IP addresses on local DNSs.
- When WINS servers are used on a network, the LMHOSTS table resolves host names to IP addresses for subnets that do not have a WINS server.

Based on the operating system installed on the client PC, sample host tables are located in varying directories. With the Windows 2000 Server installation, for example, sample host tables are provided in the following directory:

[x]:\WINNT\system32\drivers\etc

On each client PC, use a text editor to modify the host table(s) by entering the computer name and IP address of the application server.

ATTENTION

You do not have to use host tables for name resolution if the name of the application server is registered on a DNS or WINS server.

Sample host tables are provided below as a guideline, but are not intended to indicate exactly how the host tables should be configured on the client PC.

ATTENTION

Incorrectly modifying a host table on the client PC can cause extensive network problems. Before you modify any of the host tables on the client PC, you must carefully review the detailed information on HOSTS and LMHOSTS in the supporting documentation for Microsoft Windows 2000 Server.

Sample HOSTS table

The HOSTS table consists of a list of IP addresses followed by a computer name:

```
123.4.56.100 webclient.nortelnetworks.com
```

At the end of the file, type the IP address and computer name of the application server. Separate the two values by using the space or tab key.

Note: HOSTS tables are case-sensitive.

Once you edit and save the HOSTS file, the system automatically reads your new settings. If you are editing the sample HOSTS file, then save the file with no extension for the system to recognize your changes.

Sample LMHOSTS table

LMHOSTS tables are more complex than HOSTS tables. Enter keywords and comments preceded with a # sign.

```
123.45.67.89 localsrv #PRE
123.45.67.90 ptord099 #PRE #DOM:networking #net group PDC
123.45.67.100 "webclient \0x14" #Nortel app server
123.45.67.101 home #PRE #source server

#BEGIN_ALTERNATE
#INCLUDE \\localsrv\public\lmhosts #adds LMHOSTS from this
server
#INCLUDE \\ptord099\public\lmhosts #adds LMHOSTS from this
server
#END_ALTERNATE
```

Note: LMHOSTS tables are not case-sensitive.

To use the LMHOSTS file for name resolution, you must perform a series of steps on the client PC. For more information, see "To activate LMHOSTS file name resolution on the client PC" below.

To activate LMHOSTS file name resolution on the client PC

1. Click Start → Settings → Control Panel.
2. Double-click the **Network and Dial-up Connections** icon.
3. Right-click **Local Area Connection**, and then click **Properties** from the resulting pop-up menu.
4. Click **TCP/IP**, and then click **Properties**.
5. Click **Advanced**.
6. Click the **WINS** tab.
7. Click **Import LMHOSTS**.
8. Click **OK** to close the window.
9. Click **OK** twice to save your changes.

Are you having printer problems?

To print scheduled reports from the Historical Reporting component and scripts from the Scripting component, you must add and configure a local printer on the application server while logged on as the administrator. To ensure the printer was configured correctly, see “To set up a default printer” on page 178.

Note: Once the printer is configured on the application server, the administrator must remain logged on to the application server for users to access the printer.

Are you having problems upgrading Agent Desktop Displays on the client PC?

When you install Symposium Web Client 4.5 on the application server, the IIS security permissions for the MSADC virtual directory are automatically set to *Denied Access*, which prevents the automatic upgrade of Agent Desktop Displays 4.0 clients to Agent Desktop Displays 4.5. To enable the automatic upgrade to proceed, you must first set the permissions on this folder to *Granted Access*. For more information, see “To set the permissions on the MSADC folder before upgrading Agent Desktop Displays to Release 4.5” on page 355.

Are you having problems downloading third-party controls to the client PC?

If your client PC runs Windows 2000 and you are having problems downloading required third-party controls to the client PC, it may be due to the settings for the local security policy *Unsigned non-driver installation behavior.* If this policy is set to *Do not allow installation*, then you cannot install unsigned third-party controls on the client PC. For more information on this policy, and for instructions on changing its settings, see “To verify your local security policy settings” on page 310.

Application server

Are the client PCs having problems starting Symposium Web Client?

Checklist

- Ensure that the IIS service is running on the application server.
- Ensure that Active Directory is installed on the application server.
- Confirm that the event viewer logs are configured correctly on the application server. For more information, see “To configure the event viewer logs on the application server” on page 519.

To verify that IIS is running on the application server

1 On the application server, click Start → Programs → Administrative Tools → Services.

Result: The Services window appears.

2 In the right pane, locate the IIS Admin Service.

3 In the Status column, verify that this service is **Started**.

To verify that Microsoft Active Directory is installed on the application server

Click Start → Programs → Administrative Tools.

If the following programs are listed on the Administrative Tools menu, Active Directory has already been installed on the application server:

- Active Directory Domains and Trusts
- Active Directory Sites and Services
- Active Directory Users and Computers

Are you having problems communicating with Symposium Call Center Server?

- If Symposium Web Client connects to Symposium Call Center Server through a firewall, your network administrator must configure both the

router filters and the firewall to grant access to Symposium Call Center Server.

- You should also check to make sure that the Symposium Call Center Server IP address that you are using is valid.

To test application server communication with Symposium Call Center Server

If the application server cannot connect to Symposium Call Center Server, and you have already checked to make sure that the Symposium Call Center Server IP address is valid, follow these steps from the application server.

1. Ping Symposium Call Center Server.

   Contact your system administrator if you are unable to successfully ping Symposium Call Center Server.

2. Check your cabling.

3. Check the IP addresses for the application server(s) and the server(s) in Symposium Call Center Server.

4. Check the versions on servers in Symposium Call Center Server, and confirm that they are compatible with Symposium Web Client.

Using ICERTDTrace to trace IP multicast data

Real-Time Display configurations of Symposium Web Client include a diagnostic tool called ICERTDTrace.exe to assist you in determining whether your network has been configured properly for IP multicasting. If you are experiencing Real-Time Reporting or Agent Desktop Displays problems, you can also identify where the problem originates.

For example, you can use ICERTDTrace.exe to determine why real-time reporting is not displaying information on the application server after you have configured RSM on Symposium Call Center Server.

To use ICERTDTrace to trace data sent from the Symposium Call Center Server to the application server

1. At a command prompt on the application server, navigate to the Symposium Web Client folder

   C:\> **cd [*x*]:\Program Files\Nortel Networks\WClient\Server**

where [*x*] is the drive letter for the hard drive on which Windows 2000 Server is installed.

2 Enter the following command to trace data sent from Symposium Call Center Server to the application server:

ICERTDTrace -r IPreceive

Output from either of these commands is printed to the screen at run time, and to a text file called IPRcvLog.txt.

To use ICERTDTrace to trace data sent from the application server to clients

1 At a command prompt on the application server, navigate to the Symposium Web Client folder

C:\> **cd [*x*]:\Program Files\Nortel Networks\WClient\Server**

where [*x*] is the drive letter for the hard drive on which Windows 2000 Server is installed.

2 Enter the following command:

ICERTDTrace -r IPSend

Output from this command is printed to the screen at run time, and to a text file called IPSndLog.txt.

To configure the event viewer logs on the application server

If the event viewer log properties are set to the default value of overwriting events after seven days, then the event log may become full, preventing Symposium Web Client users from logging on to the application server.

To avoid this problem, after you install Windows 2000 Server with Service Pack 3 (minimum) or Service Pack 4 or later (recommended), configure each of the event viewer logs on the application server to **Overwrite events as needed** by following the instructions below.

1 On the application server, click Start → Programs → Administrative Tools → Event Viewer.

Result: The Event Viewer window appears, listing the log files on the Tree tab.

2 On the **Tree** tab, right-click the first log file, **Application Log**, and from the resulting pop-up menu, click **Properties**.

Result: The corresponding properties window appears.

3 In the Log size area of the window, select the **Overwrite events as needed** option.

4 Click **OK** to save your changes and close the properties window.

5 Perform this procedure for each of the log files in the tree.

Are you having problems with Configuration's Upload feature?

- The amount of configuration data you can upload using Symposium Web Client's Configuration component is restricted by the limits you have set in the Parameters tab of the Historical Statistics window in Symposium Call Center Server. For example, if you have a limit of 240 configured CDNs in the Historical Statistics on Symposium Call Center Server, you cannot upload more than 240 CDNs using the Symposium Configuration Tool spreadsheet. Always verify the Symposium Call Center Server limits before beginning the upload process.
- Ensure that you are uploading the template spreadsheet that you downloaded from Symposium Web Client's Configuration component. Do not upload the M1 Data Extraction Tool spreadsheet. You must copy the data from the M1 Data Extraction Tool spreadsheet into the Symposium Web Client spreadsheet template, and then upload.
- If you suspect that there are problems with the Excel application, run Detect and Repair by clicking Help → Detect and Repair. Excel searches for program defects and repairs them.
- If you are using a client PC to upload or download configuration data, try restarting the client PC. If the problems persist, try restarting the application server.
- The number of agent to skillset and agent to supervisor assignments that you can upload from the Symposium Configuration spreadsheets is restricted due to the Microsoft Excel limit of 256 columns per worksheet.

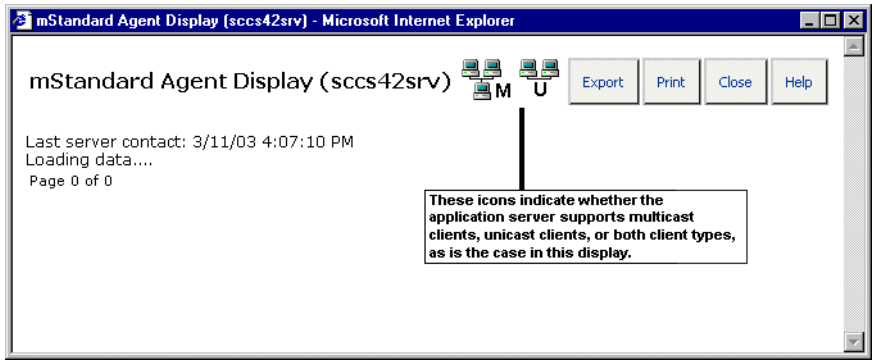
Are the real-time displays blank?

- Ensure that the LAN/WAN supports multicast traffic by contacting your network administrator to confirm that the routers have multicast capabilities.
- Verify that you can send and receive data between Symposium Call Center Server, the application server, and the application server clients. For more information, see “Using ICERTDTrace to trace IP multicast data” on page 518.
- Confirm that the RSM components are sending data to the same IP multicast address.
- Check the IP Receive address for the application server. Make sure that it matches the IP Send multicast address setting in Symposium Call Center Server. See “Modifying RSM settings and multicast rates” on page 51.

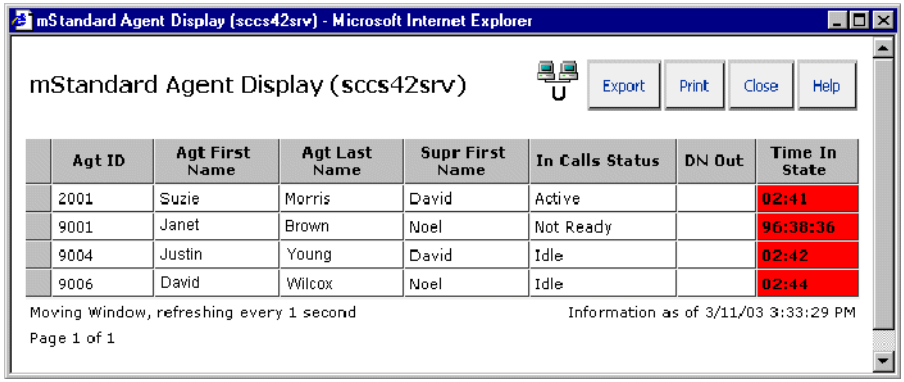
Multicast and unicast icons in real-time displays

To help you troubleshoot problems with real-time displays, when you first launch a display and while the system is retrieving data, an icon appears on the display, identifying whether the application server supports multicast clients, unicast clients, or both multicast and unicast clients.

The following graphic shows a display in which both icons are shown, indicating that the application server supports both multicast and unicast. In cases where only one transmission method is enabled, the corresponding icon appears on the display alone.



Once the display is launched, the icon indicates the transmission mode that is actually being used to launch the display. The following graphic shows a display that is receiving data through a unicast connection, a dedicated connection between the application server and client PC:



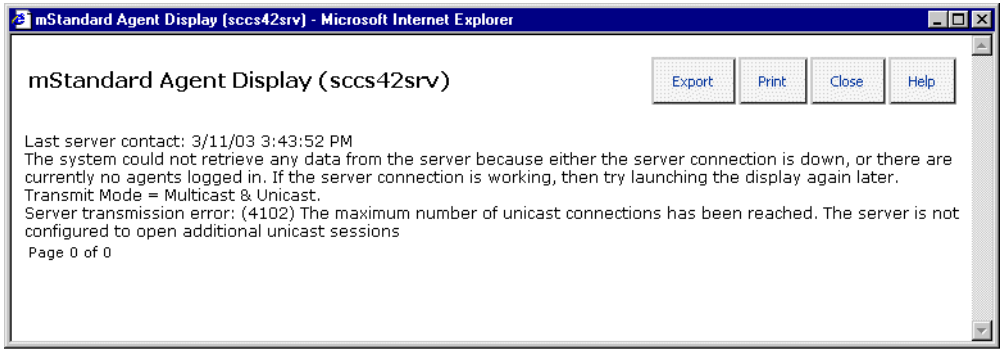
If this display were receiving multicast data, there would be a multicast icon at the top and there would be no direct connection to the application server. Instead, the client would be “listening” to a shared multicast data stream.

There are a number of reasons why the real-time displays can appear blank, as described in the following scenarios:

No unicast sessions available

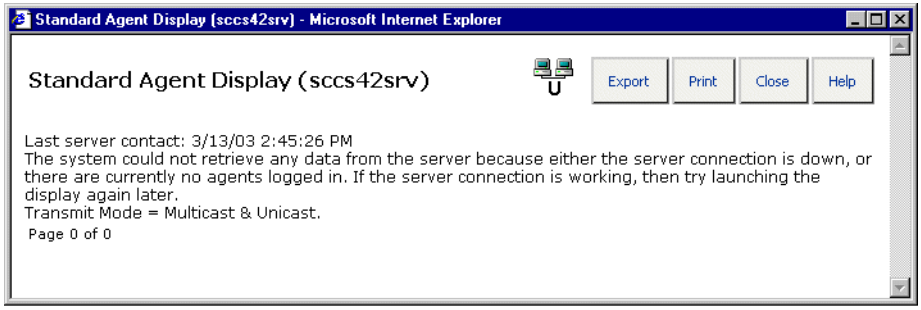
This error normally appears on a client computer when an attempt to open a unicast channel fails and the client is not receiving multicast data. From the error message shown in the following graphic, you can see that the application server supports both multicast and unicast clients, so the implication is that this client is on a unicast-only segment of the network. The absence of a unicast icon indicates that the unicast connection was not successfully established and the client PC is not receiving data packets. In this case, close the display and try to launch it again later.

Note: In this case, close the display and try to launch it again later. If the problem persists, you may need to increase the number of unicast connections that the application server allows (subject to prior engineering analysis).



No relevant data

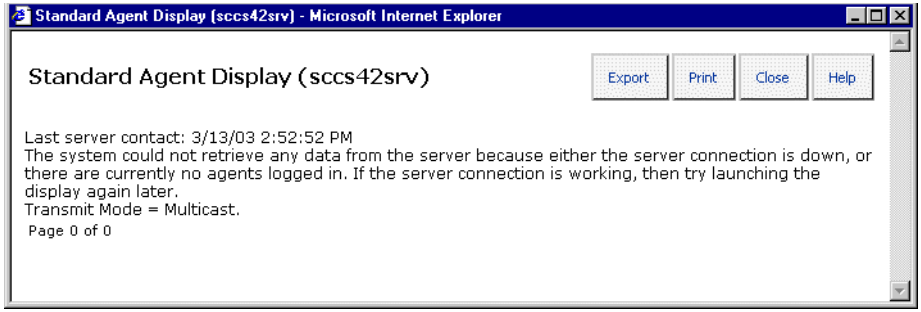
The following window appears on a client computer when it is receiving data, but the data is not relevant for the current display (for example, when the information is not available within the user's partition(s) or the current filter blocks the data from the display). The presence of the unicast icon indicates that a unicast connection was successfully established and the client PC is receiving data packets.



No data is available on the network

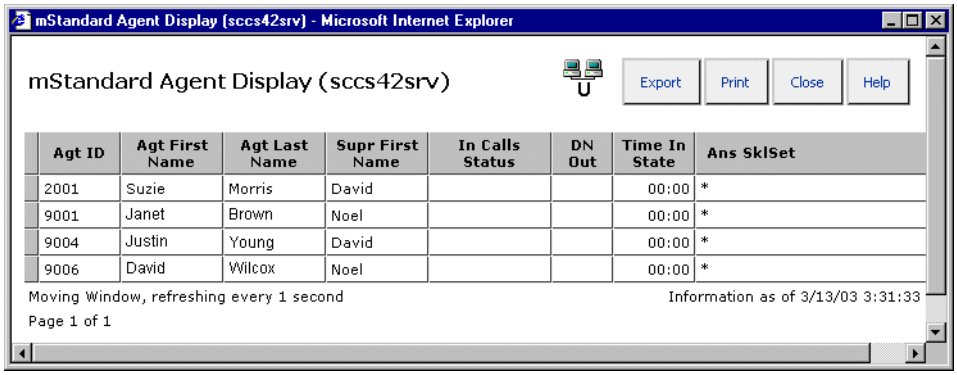
This window appears on a client PC when it is not receiving any data. There is no icon at the top of the window, indicating that the display is not receiving any data. The *Transmit Mode = Multicast* note implies that the server only supports multicast, but, in this case, the client PC is not receiving multicast data. This may be the result of a network problem, or it may mean that the server should

support unicast, but it has not been enabled. Report the problem to your administrator so that he or she can check the application server settings and enable unicast, if necessary. The administrator may also check the network settings to determine why the client PCs cannot receive multicast data.



The characters “*” and “0” appear in the display

Occasionally, the statistics in a real-time display may stop updating and the characters “*” and “0” appear instead of the variable fields, as shown in the following graphic. In a unicast environment, this indicates that the server has stopped sending data to this client. You must close and reopen the display. In a multicast environment, this indicates that the server may have stopped sending the multicast stream. Run a trace on the application server if the problem persists.



Are you having problems with Active Directory?

Nortel Networks recommends that you install the Windows 2000 support tools for troubleshooting problems with Active Directory.

To Install Windows 2000 support tools

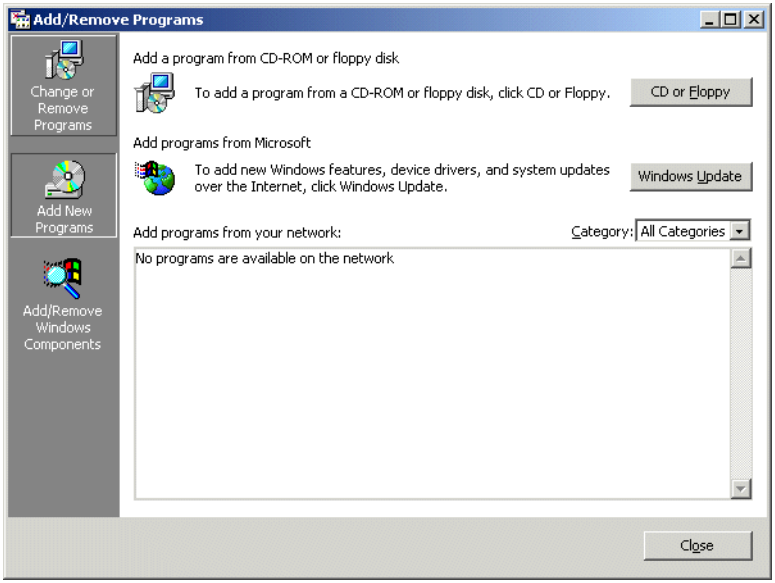
1 Insert the Microsoft 2000 CD in the application server's CD-ROM drive.

2 Click Start → Settings → Control Panel.

Result: The Control Panel window appears.

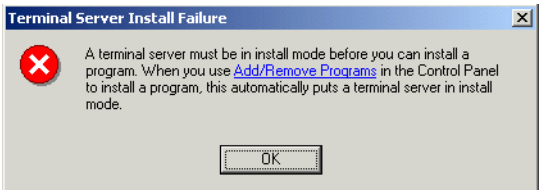
3 Click **Add/Remove Programs**.

Result: The Add/Remove Programs window appears.

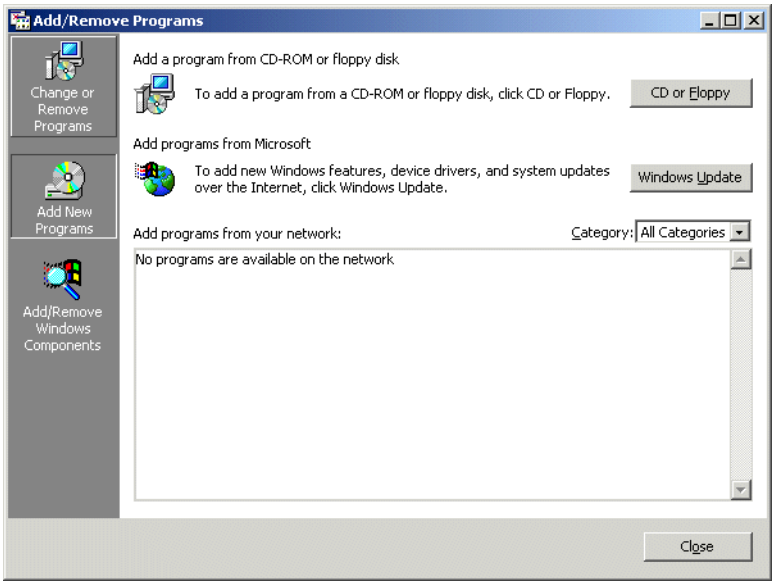


Note: If you double-click the setup.exe file on the Symposium Web Client CD, or if the setup file launches automatically, the Terminal Server Install

Failure dialog box appears. This occurs because Terminal Services must be in Install Mode before you can install an application.



To switch Terminal Services to Install Mode and install the Windows 2000 support tools, select the Add/Remove Programs link in the dialog box. The Add/Remove Programs window appears, and Terminal Services automatically switches to Install Mode.



4 Click **Add New Programs**.

5 Click **CD or Floppy** to indicate that you want to install the Windows 2000 support tools from the CD-ROM.

Result: The Install Program From Floppy Disk or CD-ROM window appears.

6 Click **Next**.

Result: The Run Installation Program window appears.

7 Click **Browse,** and then navigate to D:\Support\Tools\setup.exe, where D: is the application server's CD-ROM drive.

8 Click **OK**.

Result: The Windows 2000 Support Tools Setup Wizard window appears.

9 Click **Next**.

Result: The User Information Window appears.

10 In the **Name** box and the **Organization** box, enter the appropriate information.

11 Click **Next**.

Result: The Select An Installation Type window appears.

12 Click **Typical**.

13 Click **Next**.

Result: The Begin Installation window appears.

14 Click **Next**.

Result: After the system copies files to the application server, the Completing the Windows 2000 Support Tools Setup Wizard window appears.

15 Click **Finish**.

Result: The After Installation window appears.

16 Click **Next**.

Result: The Finish Admin Install window appears.

17 Click **Finish**.

Did you configure a name resolution server?

If you did not configure a name resolution server, such as a DNS server, during the Windows 2000 Server installation, Symposium Web Client cannot find the Symposium Call Center Server systems. In this case, your next step is to manually update the HOSTS or LMHOSTS tables.

When you use server names to connect to an application server in TCP/IP networks, the server name must be associated with an IP address. LMHOSTS and HOSTS are host tables that carry out this association, which is called name resolution.

- The HOSTS table resolves host names to IP addresses on local DNS servers.
- When WINS servers are used on a network, the LMHOSTS table resolves host names to IP addresses for subnets that do not have a WINS server.

Sample host tables are provided with the Windows 2000 Server installation in the following directory:

[x]:\WINNT\system32\drivers\etc

Use a text editor to modify the host table(s), and to enter the name and IP address of

- each Symposium Call Center Server
- each NCC Server

ATTENTION

You do not have to use host tables for name resolution if the names of the servers in Symposium Call Center Server and the NCC server names are registered on a DNS or WINS server.

Sample host tables are provided below as a guideline, but are not intended to indicate exactly how the host tables should be configured on the application server.

ATTENTION

Incorrectly modifying a host table on the application server can cause extensive network problems. Before you modify any of the host tables on the application server, you must carefully review the detailed information on HOSTS and LMHOSTS in the supporting documentation for Microsoft Windows 2000 Server.

Sample HOSTS table

The HOSTS table consists of a list of IP addresses followed by a computer name:

```
123.4.56.100 webclient.nortelnetworks.com
```

At the end of the file, type the IP address and computer name of the servers that you are adding to the file. Separate the two values by using the space or tab key.

Note: HOSTS tables are case-sensitive.

Once you edit and save the file, the system automatically reads your new settings. If you are editing the sample HOSTS file, then save the file with no extension for the system to recognize your changes.

Sample LMHOSTS table

LMHOSTS tables are more complex than HOSTS tables. Enter keywords and comments preceded with a # sign.

```
123.45.67.89 localsrv #PRE
123.45.67.90 ptord099 #PRE #DOM:networking #net group PDC
123.45.67.100 "webclient \0x14" #Nortel app server
123.45.67.101 home #PRE #source server

#BEGIN_ALTERNATE
#INCLUDE \\localsrv\public\lmhosts #adds LMHOSTS from this
server
#INCLUDE \\ptord099\public\lmhosts #adds LMHOSTS from this
server
#END_ALTERNATE
```

Note: LMHOSTS tables are not case-sensitive.

You must click the Import LMHOSTS option on the WINS Address tab in TCP/IP properties in the Network option to use the LMHOSTS file for name resolution.

Before you can use the LMHOSTS file for name resolution, you must perform a series of steps on the application server. For more information, refer to “To activate LMHOSTS file name resolution,” on page 530.

To activate LMHOSTS file name resolution

1. Click Start → Settings → Control Panel.
2. Double-click the **Network and Dial-up Connections** icon.
3. Right-click **Local Area Connection**, and then click **Properties** from the resulting pop-up menu.
4. Click **TCP/IP**, and then click **Properties**.
5. Click **Advanced**.
6. Click the **WINS** tab.
7. Click **Import LMHOSTS**.
8. Click **OK** to close the window.
9. Click **OK** twice to save your changes.

Simple Object Access Protocol errors

Are you receiving Simple Object Access Protocol errors?

When you investigate Simple Object Access Protocol (SOAP) errors, you must check the settings and configuration on both the application server and the client PCs. This section is separated into the actions that you perform on each type of computer.

Application server

If you are receiving Simple Object Access Protocol (SOAP) errors, check the following on the application server:

1. Ensure that the application server is set up as a Trusted Site that allows the downloading of signed ActiveX Controls. For details, see “To configure Internet Explorer 5.5 Service Pack 2 (or later)” on page 294, or “To configure Internet Explorer 6.0 Service Pack 1 (or later)” on page 297.
2. Check for the required files on the application server, as follows:

- In the following path,

  C:/Program Files/Common Files/MSSOAP/Binaries

  where *C* is the drive on which SOAP is installed, ensure that these required SOAP .dll files exist:
  - MSSOAP30.dll
  - SOAPIS30.dll
  - WHSC30.dll
  - WISC30.dll
- In the following path,

  C:/Program Files/Common Files/MSSOAP/Binaries/Resources/1033

  where *C* is the drive on which SOAP is installed, ensure that this required SOAP .dll file exists:
  - MSSOAPR30.dll
- In the following path,

  C:/WINNT/System32

where *C* is the drive on which the operating system is installed, ensure that the following Microsoft XML parser files exist:

- msxml4.dll
- msxml4r.dll

3. Ensure that the application server is registered with the DNS server by logging on to Symposium Web Client using the application server name, instead of the IP address.

   a. On the application server (or on a client PC), open Internet Explorer.

   b. In the **Address** box, type the URL of your application server, using the appropriate protocol for your network (either HTTP or HTTPS).

   Result: If the server is registered with the DNS server, then the Symposium Web Client Logon page appears. If an error message appears, then the server name is not registered with the DNS server.

4. Ensure that the appropriate SOAP files are using the application server name as follows:

   a. Navigate to the location where Symposium Web Client is installed:

   X:/Program Files/Nortel Networks/WClient/Apps/Common/SOAP

   b. Use a text editor, such as Notepad, to open the WSDL file, *SOAPWrapper.WSDL*.

   c. Scroll down to the end of the file and ensure that the port address does *not* reference *localhost*, but the application server name.

Example

The following line shows an example where the port address references the localhost, which is the wrong configuration for Symposium Web Client:

*<soap:addresslocation='http://**localhost**/SWCCommon/SOAP/SOAPWrapperCommon.ASP'/>*

If you see the above configuration, then you must replace *localhost* with the computer name of the application server. In the following example, the computer name of the application server is *SWCCONFIG*:

*<soap:addresslocation='http://**SWCCONFIG**/SWCCommon/SOAP/SOAPWrapperCommon.ASP'/>*

5. Ensure that IIS is configured correctly, as follows:

   a. Click Start → Programs → Administrative Tools → Internet Services Manager.

   b. In the Internet Information Services window, click the plus sign (+) beside the server name.

   c. In the tree, right-click **Default Web Site**, and then click **Properties** from the resulting pop-up menu.

   d. Click the **Home Directory** tab.

   e. Click **Configuration**.

   f. On the **App Mappings** tab, in the Application Mappings box, verify whether the .wsdl extension appears under the **Extension** column heading.

   g. If this value exists, then it references the SOAPISAP.dll at the location *C:/Program Files/Common Files/MSSoap/Binaries/SOAPISAP.dll*.

   h. Highlight this line, and then click **Remove**.

   i. Click **OK** twice to save your changes.

   j. Close the Internet Information Services window.

   k. Restart IIS to register your new changes.

6. Ensure that the system can load the WSDL file, as follows:

   a. Open Internet Explorer.

   b. In the Address box, type the location of the WSDL file:

   http://servername/Common/SOAP/SOAPWrapper.WSDL, where *servername* is the computer name of the application server.

   c. Press **Enter**.

   Result: The WSDL file should appear in XML format. If the system cannot load the file in this format, then an error message appears.

Client PC

If you are receiving Simple Object Access Protocol (SOAP) errors, check the following on the client PC:

1. Ensure that the application server is set up as a Trusted Site that allows the downloading of signed ActiveX Controls. For details, see “To configure Internet Explorer 5.5 Service Pack 2 (or later)” on page 294, or “To configure Internet Explorer 6.0 Service Pack 1 (or later)” on page 297.
2. Ensure that ClientSoap.msi is installed. To verify if it is installed, ensure that all the SOAP and Microsoft XML parser files noted on page 531 are in the same locations on the client PC.

Notes:

- The file WHSC30.dll only appears on client PCs running Windows 2000 Server, Windows XP, and Windows NT 4.0 Workstation. If the client PC runs on any other platform, then this file is not applicable.
- If the client PC runs on Windows 98, then the C:/WINNT/System32 folder does not exist. In this case, the XML parser files *msxml4.dll* and *msxml4r.dll* are located in the folder C:/Windows/System.

3. If ClientSoap.msi is not installed, then a message appears when you first attempt to log on to Symposium Web Client, giving you the option of downloading the Client Soap package from the application server. You must have administrative privileges to install this package.

Appendix A

Installation worksheets and checklists

In this appendix

Overview 536

Pre-installation worksheet 537

Installation checklist 545

Windows 2000 Server/Advanced Server installation checklist 550

Overview

Introduction

Before installing Windows 2000 Server/Advanced Server and Symposium Web Client, Nortel Networks recommends that you complete the “Pre-installation worksheet” on page 537. This worksheet lists tasks and information that you need to complete or gather before the installation.

Also, during the installation, you must install and configure software in a precise order on the server in Symposium Call Center Server, on the Web Client application server, and on client PCs. Follow the order listed in the “Installation checklist” on page 545 to ensure that Symposium Web Client functions properly upon completion of the installation.

ATTENTION

When installing and configuring the software on the application server, you cannot install a non-English version of the operating system over a previously installed English version of the operating system. Instead, you must ensure that the application server is completely clean and free of all English operating system components before proceeding with the non-English installation. Failure to do so results in functionality problems in Symposium Web Client.

Pre-installation worksheet

	Pre-installation questions	Fill in the required information
1	Computer name that will be assigned to the application server? **Note:** The computer name can be a maximum of 12 characters only.	
2	IP address for the application server?	
3	Name of the domain for the application server? **Note:** Before you choose the domain name for the application server, consult with your LAN administrator to ensure that it adheres to the naming conventions established for your network. You cannot change the domain name after you install Symposium Web Client. To change the domain name, you must uninstall and reinstall the software with the new name.	
4	Subnet that the application server belongs to?	

	Pre-installation questions	Fill in the required information
5	Is the computer name of the application server registered with the DNS server? From the client PC, type **ping -a *app-server-ip-address***. The system must return the same name that is registered with the DNS server for the application server. If the computer names do not match, you must resolve the conflict before proceeding.	
6	Default gateway that the application server will use?	
7	Are the unique CLAN IP addresses of each Symposium Call Center Server system registered with Domain Name Services (DNS)?	
8	Is the physical computer name of each Symposium Call Center Server registered with the DNS server? From the application server, type **ping -a *CLAN IP address***. The system must return the same name that is registered with the DNS server for each Symposium Call Center Server. If the computer names do not match, you must resolve the conflict before proceeding.	
9	IP address for the Preferred DNS server (to enable forward/reverse lookups)?	
10	IP address for the Alternate DNS server?	

	Pre-installation questions	Fill in the required information
11	What is the name and CLAN IP address of ■ each Symposium Call Center Server system? ■ Network Control Center (NCC) server? This information must be entered in the HOSTS or LMHOSTS tables if the CLAN IP addresses of each Symposium Call Center Server system are *not* registered with the DNS. For more information, refer to "Did you configure a name resolution server?" on page 527. You also require this information when you first configure your call center using Symposium Web Client.	
12	The number of concurrent connections that will be established between clients and the application server to allow the application server to communicate with other networks/ subnetworks?	
13	Is the network connection between the client PCs and the application server multicast-capable?	
14	IP multicast address that Symposium Call Center Server is using to send data to Symposium Web Client? (This IP multicast address will also be used as the application server's receiving IP multicast address.)	

	Pre-installation questions	Fill in the required information
15	The IP multicast address that the application server will use to send Real-Time Reporting and Agent Desktop Displays data to its clients?	
16	The IP multicast address that the application server will use to send Emergency Help data to its clients (if different than the address used to send Real-Time Reporting and Agent Desktop Displays data)? **Note:** The application server can have two different IP Send addresses: one used to send Real-Time Reporting and Agent Desktop Displays data to client PCs, and another used to send Emergency Help data to client PCs. You can use two different IP addresses, or you can use one IP Send address for both types of data.	
17	Has Real-time Statistics Multicast (RSM) been enabled on Symposium Call Center Server? For more information, refer to Chapter 2, “Preparing Symposium Call Center Server”	
18	Have you modified the default RSM settings on Symposium Call Center Server? For more information, refer to “Modifying Real-time Statistics Multicast settings” on page 49.	

	Pre-installation questions	Fill in the required information
19	What multicast rate (the default rate is 5 seconds) are you going to use? For more information, refer to “Modifying RSM settings and multicast rates” on page 51.	
20	What is the Time-To-Live setting for RSM? For more information, refer to “Modifying RSM settings and multicast rates” on page 51.	
21	Which real-time statistics are you going to collect? **M1/CSE 1000** (skillset, application, agent, nodal, route, IVR) **DMS/MSL-100** (skillset, application, agent, nodal) For more information, refer to “Modifying RSM settings and multicast rates” on page 51.	
22	What is the name of your mail server? You must enter this information if you are configuring automatic e-mail notification in the Historical Reporting component. See “Configuring Historical Reporting” on page 175.	

	Pre-installation questions	Fill in the required information
23	Which e-mail address should be used for notification of Non-delivery reports? You must enter this information if you are configuring automatic notification of the Non-Delivery report in Historical Reporting. See “Configuring Historical Reporting” on page 175.	
24	What is the name and IP address of the printer you will be using for Historical Reporting and Scripting? See “To set up a default printer” on page 178.	

	Pre-installation questions	Fill in the required information
25	How many client PCs will require access to the Script Manager component (for script editing)? **Note:** As of date of publication, the following information on Client Access Licensing was available from Microsoft. Consult Microsoft for the latest information. Nortel Networks does not accept any liability for end-user compliance with Microsoft licensing agreements. This information has been provided for your convenience. ■ You must purchase from Microsoft both a Terminal Services Client Access License and a Windows 2000 Server Client Access License for each client PC running on Windows 98 or NT that will be accessing the Script Manager portion of the Scripting component. ■ Client PCs running on Windows 2000 or Windows XP require a Windows 2000 Server Client Access License only; they do not require a separate Terminal Services Client Access License. ■ Nortel Networks does not provide these Client Access Licenses. ■ The Windows 2000 Server Client Access Licenses do not float (that is, they are specific to the client PCs for which they have been purchased). ■ If the client PC is accessing only Script Variables or Application Thresholds, then these licenses are not required.	

	Pre-installation questions	Fill in the required information
26	Is Internet Explorer configured on client PCs to use a Proxy Server? If so, notify your Proxy Server administrator to avoid any potential browsing problems.	
27	Have you downloaded the most recent Service Update for Symposium Call Center Server and Symposium Web Client from https://www21.nortelnetworks.com/MPL (for Europe), or from https://www43.nortelnetworks.com/MPL (for North America)?	

Installation checklist

Install order	Installation task description	✓
Symposium Call Center Server		
1	Configure the Real-Time Statistics Multicast (RSM) component on each server in Symposium Call Center Server that provides real-time statistics. For more information, refer to Chapter 2, “Preparing Symposium Call Center Server”	❑
2	Test the Real-Time Statistics Multicast service. For more information, see “Testing the Real-time Statistics Multicast service” on page 58.	❑
3	Download and apply the latest Service Update for Symposium Call Center Server from https://www21.nortelnetworks.com/MPL (for Europe), or from https://www43.nortelnetworks.com/MPL (for North America). Then check to see if there are any updates posted in installation addenda on either http://www.nortelnetworks.com (for end customers), or http://www.nortelnetworks.com/prd/picinfo/ (for distributors).	❑

Install order	Installation task description	✓
Application Server		
4	Install Windows 2000 Server/Advanced Server with SMTP, Internet Information Services (IIS),Terminal Services, and Terminal Services Licensing. For more information, refer to "Windows 2000 Server/Advanced Server installation checklist" on page 550. **Note:** After you have finished installing all software on the application server, you must activate the Terminal Services License Server. For more information, see "To activate the Terminal Services License Server" on page 192. **Note:** Terminal Services can communicate with the Terminal Services License Server (Terminal Services Licensing) only if they are in the same domain. Therefore, Nortel Networks recommends that you install both on the application server because it is a domain controller.	❑
5	Install Windows 2000 Server Service Pack 3 (minimum), Service Pack 4 or later (recommended) if it was not installed during the Windows 2000 installation. **Note:** A Microsoft Windows 2000 memory leak fix is included in Windows 2000 Server Service Pack 2. Therefore, you must install this Service Pack or later on the application server.	❑
6	Install Microsoft Active Directory. For more information, refer to "Installing Microsoft Active Directory" on page 75.	❑
7	Install the third-party application, Sybase Open Client v.12.5, for the Historical Reporting and Contact Center Management components. For more information, refer to "Installing Sybase Open Client on the application server" on page 88.	❑
8	Install Symposium Web Client. For more information, refer to "Installing Symposium Web Client on the application server" on page 98.	❑

Install order	Installation task description	✓
9	Download and apply the latest Service Update for Symposium Web Client from https://www21.nortelnetworks.com/MPL (for Europe), or from https://www43.nortelnetworks.com/MPL (for North America). Then check to see if there are any updates posted in installation addenda on either http://www.nortelnetworks.com (for end customers), or http://www.nortelnetworks.com/prd/picinfo/ (for distributors).	❑
10	Upgrade Microsoft Internet Explorer from version 5.0 to version 5.5 Service Pack 2 (or later). For more information, see “Upgrading Internet Explorer on the application server” on page 113. **Note:** Internet Explorer Service Pack 2 (minimum) or Internet Explorer 6.0 or later (recommended) is required so support personnel can access the application server.	❑
11	Configure Real-Time Reporting, including the multicast and unicast settings. For more information, see “Configuring Real-Time Reporting” on page 165.	❑
12	Configure Emergency Help. For more information, refer to “Configuring Emergency Help” on page 173.	❑
13	Configure SMTP on the application server (if you are using the Historical Reporting component). For more information, refer to “Configuring Historical Reporting” on page 175.	❑
14	Configure Terminal Services on the application server. For more information, refer to “Configuring Scripting” on page 183. **Note:** While configuring Terminal Services, you must activate the Terminal Services License Server on the application server. For more information, see “To activate the Terminal Services License Server” on page 192.	❑

Install order	Installation task description	✓
15	Configure Agent Desktop Displays' server component (if Agent Desktop Displays is going to be used on a client). For more information, refer to "Configuring Agent Desktop Displays" on page 194.	❑
16	Configure the application server for optimum security. To do so involves removing the Windows 2000 Everyone group, and, optionally, changing the default Anonymous Internet Guest account, disabling the parent path in IIS, and enabling Secure Sockets Layer. For more information, see Section F: "Security and the application server," on page 197.	❑
17	Optionally, install the automated assignments feature. For more information, see the *XML Assignments User Guide*. This guide, and other associated documentation and engineering/development support resources for the XML automated assignments feature, are provided only through the Nortel Networks Developer Program. For information on obtaining the XML Automated Assignment toolkit, contact a member of the Developer Program through the Contact Us link on their web site at http://www.nortelnetworks.com/developer. General information on the Developer Program, including an online membership application, is also available on this site.	❑
18	Optionally, if you want to use a localized version of Symposium Web Client, install the appropriate language pack and configure the server for this language. For more information, see "Overview of steps for configuring multiple language support" on page 129.	❑
Client Workstation		
19	Install any required third-party applications. **Note:** The third-party applications that must be installed on a client vary depending on the client's operating system. For more information, refer to "Installing third-party software on a client" on page 288.	❑

Install order	Installation task description	✓
20	Configure Internet Explorer. For more information, see "To configure Internet Explorer 5.5 Service Pack 2 (or later)" on page 294, or "To configure Internet Explorer 6.0 Service Pack 1 (or later)" on page 297.	❑
21	Install Agent Desktop Displays on client PCs.	❑

If you experience technical difficulties while installing Symposium Web Client, ensure that you have downloaded the latest Service Updates and Performance Enhancement Packages (PEPs) for Symposium Call Center Server and for Symposium Web Client. You can access the most recent updates and any changes posted in installation addenda from https://www21.nortelnetworks.com/MPL (for Europe), or from https://www43.nortelnetworks.com/MPL (for North America).

Note: To register for either of these web sites, follow the instructions listed at http://nortelnetworks.com/register.

Nortel Networks personnel use pcAnywhere only as a remote support tool. If you require remote support from Nortel Networks, it is recommended that you install pcAnywhere v.10.5. For more information, see "To install pcAnywhere 10.5" on page 503.

Windows 2000 Server/Advanced Server installation checklist

ATTENTION

To minimize the risk of post-installation issues due to misconfiguration, Nortel Networks recommends that you install the operating system from the original operating system CD-ROM, following the instructions in this installation checklist. If you choose to install the operating system from a ghost image, then you must ensure that the image is taken from an installation where all instructions in the following checklist have been followed. Installations from a ghost image of the operating system, where the instructions in the following checklist were not followed, can result in problems that are difficult to diagnose and can delay the commissioning of Symposium Web Client.

The following checklist describes the Windows 2000 Server/Advanced Server installation order:

Windows 2000 Server/Advanced Server installation checklist	✓
Set up a partition on the application server with an NTFS file system on the partition that will contain the Web Client application. **ATTENTION** If you are unfamiliar with formatting hard drives, setting up partitions, and selecting file systems, see your Microsoft Windows 2000 Server/Advanced Server documentation for more information before you perform this procedure. Failure to do so may result in loss of data.	❑

Windows 2000 Server/Advanced Server installation checklist	✓
After creating the partition, the system copies Windows 2000 Server/Advanced Server files to the hard drive. When the copy process is complete, the system restarts.	❑
Windows 2000 Server/Advanced Server displays the following windows: ■ a system devices (mouse, keyboard, monitor, and so on) installation window ■ a regional settings window in which you can customize the system for your current geographical region ■ an identification window in which you can enter your name and the name of your organization	❑
Licensing Modes window The following settings are recommended in this window: ■ Click **Per Server**. ■ Type **5*** in the **Concurrent Connections** box. *See Note. **Note:** The number that you type in this box must be equal to at least the number of Terminal Services Client Access Licenses (CALs) that you have purchased. The number of script editing sessions allowed depends on the number of Windows 2000 Server/Advanced Server CALs and Terminal Services CALs that you have purchased, whichever is lower (*each* client accessing Scripting requires both of these types of licenses; however, you may have other client workstations in your network that only have Windows 2000 Server/Advanced Server CALs and do not require access to Scripting).	❑

Windows 2000 Server/Advanced Server installation checklist	✓
Computer Name and Administrator Password window 1 The system displays a computer name. Change this name to match the computer name supplied to you by the network administrator. This information should be recorded in the "Pre-installation worksheet" on page 537. 2 Type the password for the Administrator account for this computer. You must use this password whenever the user name *Administrator* is used to log on to the computer on which Symposium Web Client resides. **WARNING** You cannot change the computer name that you choose during the Windows 2000 Server/Advanced Server installation at a later date without disrupting the operations of both Symposium Web Client and Active Directory. Both applications require the computer name to be identified on the network.	❑

Windows 2000 Server/Advanced Server installation checklist	✓
Windows Components window Accept the default values in this window, and click Terminal Services and Terminal Services Licensing. Terminal Services is required for Symposium Web Client's Scripting component. SMTP is a subcomponent of IIS and is checked by default. Click **Internet Information Services**, and then click **Details** to see SMTP on the components list. **Note:** As of date of publication, the following information on Client Access Licensing was available from Microsoft. You must consult Microsoft for the latest information. Nortel Networks does not accept any liability for end-user compliance with Microsoft licensing agreements. This information has been provided for your convenience. ■ You must purchase from Microsoft both a Terminal Services Client Access License and a Windows 2000 Server Client Access License for each client PC running on Windows 98 or NT that will be accessing the Script Manager portion of the Scripting component. ■ Client PCs running on Windows 2000 or Windows XP require a Windows 2000 Server Client Access License only; they do not require a separate Terminal Services Client Access License. ■ Nortel Networks does not provide these Client Access Licenses. ■ The Windows 2000 Server Client Access Licenses do not float (that is, they are specific to the client PCs for which they have been purchased). ■ If the client PC is accessing only Script Variables or Application Thresholds, then these licenses are not required.	❑
Date and Time Settings window Adjust as required.	❑

Windows 2000 Server/Advanced Server installation checklist	✓
Terminal Services Setup windows 1 Click **Application Server mode**. 2 Click **Next**. 3 Click **Permissions Compatible With Terminal Server 4.0 Users**.* 4 Click **Next**. 5 Restart the server, if prompted to do so. *If *all* of the application server's client PCs are running on the Windows 2000 Professional platform, you can click **Permissions Compatible With Windows 2000 Users**.	❑
Network Settings window 1 Click **Custom Settings**. 2 Click **Next**. The Networking Components window appears.	❑

Windows 2000 Server/Advanced Server installation checklist	✓
Networking Components window Use this window to set up subnets, gateways, and domain names. **Note:** Before you choose the domain name for the application server, consult with your LAN administrator to ensure that it adheres to the naming conventions established for your network. You cannot change the domain name after you install Symposium Web Client. To change the domain name, you must uninstall and reinstall the software with the new name. 1 Click **Internet Protocol (TCP/IP)**, and then click Properties. The Internet Protocol (TCP/IP) Properties window appears. **Note:** Do not use dynamic IP addressing. 2 Click **Use the following IP address**, and, in the IP address section, enter the IP address for the application server, the subnet mask, and default gateway that your company uses. 3 Click **Use the following DNS server addresses**, and then enter the IP address for the Preferred DNS server and Alternate DNS server. 4 Click **Advanced**. The Advanced TCP/IP Settings window appears.	❑

Windows 2000 Server/Advanced Server installation checklist	✓
Advanced TCP/IP Settings window 1 Click the **DNS** tab. 2 In the lower half of the window, click **Append these DNS suffixes**, and then click **Add**. Type the suffixes that your company uses (for example, ca.softwaremaker.com). 3 If your company uses Windows Internet Naming Services (WINS) or programs that require the NetBIOS protocol, do the following: ■ Click the WINS tab. ■ Type the WINS IP address, and then click **Add** to add it to the list. Click **OK**. 4 Click **OK** to close the General TCP/IP Settings window. 5 Click **Next**. The Workgroup or Computer Domain window appears.	❑
Workgroup or Computer Domain window **Note:** You must set up the application server as a stand-alone server. 1 Click **No, this computer is not on a network, or is on a network without a domain**. 2 Click **Next**. The Installing Components window appears.	❑
Installing Components window The Windows 2000 Server Setup Wizard continues with the installation, copying the files required for the settings you have selected.	❑
Performing Final Tasks window In this window, Setup registers components, installs Start menu components, and removes temporary files.	❑

Windows 2000 Server/Advanced Server installation checklist	✓
Upgrading to Windows 2000 Service Pack 3 or later After you install Windows 2000 Server, you must upgrade to Service Pack 3 (minimum) or Service Pack 4 or later (recommended) if it was not installed during the Windows 2000 installation. **Note:** A Microsoft Windows 2000 memory leak fix is included in Windows 2000 Server Service Pack 2. Therefore, you must install this Service Pack or later on the application server. If you do not have Service Pack 3 or later, you can download the files from Microsoft's web site, or install the files from the CD-ROM.	❑
Creating shared folders on the application server After you install Windows 2000 and upgrade to Service Pack 3 or later, create the shared folders and add the printers on the application server that will be used for Scripting and Historical Reporting. For more information, see "Configuring Historical Reporting" on page 175, and "Configuring Scripting" on page 183.	❑

Appendix B

IP Multicast Networking

In this appendix

Overview 560

Multicast sending and receiving 561

Implementing IP multicasting for Symposium Web Client 571

Overview

Introduction

What is IP multicasting?

IP multicasting provides multipoint communication by simultaneously delivering information from one sender to multiple receivers who want to receive the information. The greatest advantage to IP multicasting is its ability to transmit information to many recipients in a way that minimizes the bandwidth required to communicate across networks, and the resources required by the sender to carry out a transmission.

Traditional multipoint communications

Traditional methods of multipoint communication require that a source send a copy of information to each recipient: ten recipients require ten copies of the data. This method, called point-to-point unicast, creates two constraints:

- The source's system resources are used up in the duplication and distribution of multiple copies of a single piece of information.
- The combined size of the copies of data sent to recipients cannot be greater than the share of bandwidth available to the source.

IP multicasting multipoint communications

Both point-to-point unicast and broadcast communications are server-based concepts that negatively impact the source system and its network.

With IP multicasting, communication is receiver-based. Users who want to receive data join a multicast host group and become members of that group. Since duplication and distribution of the information is handled by a router, the source computer's resources and its designated bandwidth are utilized efficiently, allowing the source to distribute information quickly and with minimal impact on the network.

Multicast sending and receiving

Introduction

To send to multiple users, IP multicasting communicates with multicast host groups that are comprised of multicast group members. Recipients must be members of multicast groups to receive multicast data. A sender, however, does not need to be a member in a multicast host group to transmit multicast data. Anyone who can send information to a multicast IP address can send multicast information to a multicast host group. The following sections look at the building blocks of multicast communication in greater detail.

How sending and receiving works

Multicast IP sending is the same as unicast sending: the sender indicates the IP address that it wants to send to, and the information travels through the network and arrives at its destination.

Receiving multicast IP datagrams is more complex. When an application on a PC indicates that it wants to receive multicast data, several things must occur in the background for the data to travel through the network(s) and be received by the application. The section below looks at sending and receiving within the framework of Symposium Web Client's Real-Time Reporting component.

Sending

Sending begins when a user opens a browser, connects to the Symposium Web Client application server, and opens Real-Time Reporting. Real-Time Reporting on the client issues a request to join a host member group associated with Real-Time Reporting multicast data. The request is sent to the host member group's multicast group host.

Note: When a multicast host group is part of a permanent group, the host filters continuously for data coming from the multicast IP address. If the host is dynamic, it only begins filtering for data when it receives a request for membership. See "Multicast host groups," on page 564 for more information on the types of multicast groups.

In IP multicasting, there is an All-Hosts Group with the reserved address 224.0.0.1, whose function is to represent all hosts on the network. The All Routers Group with the reserved multicast IP address 224.0.0.2 represents the communication point for all routers on the network. The All-Hosts Group continuously sends out requests to its hosts and asks for a report: “Are there any groups that contain members who want to receive multicast data?”

Since the concept of IP multicasting rests upon the idea of virtual networks, an All-Hosts Group should be viewed only as representing all of the host groups, not a physical piece of hardware. The address 224.0.0.1 can designate

- a router

  or

- a system with an IP multicast-capable network interface card

If you are using IP multicasting in a very simple network, one router on a LAN can represent

- the All-Hosts Group
- the All-Routers Group

  and

- the host that the host group members join to receive their multicast data

In this example, the network consists of two servers in Symposium Call Center Server on one LAN. The Symposium Web Client application server and its client PCs reside on a separate LAN. Each server in Symposium Call Center Server and the Symposium Web Client application server are connected to multicast routers.

In this scenario, one of the routers is designated as the All-Routers Group (224.0.0.2). The Symposium Web Client application server acts as the host to the host group members, while one of the Symposium Call Center Server routers acts as the All-Hosts Group (224.0.0.1). At this stage, the All-Hosts group waits to find out if there are hosts with members who want to receive multicast data.

The All-Hosts Group sends a query requesting that its hosts report on its membership, and the query travels from the All-Hosts Group to the host(s).

The host(s) report on their membership lists. These are all of the clients who requested membership in a host group by opening a browser, launching Web Client, and then opening Real-Time Reporting.

The report travels from each host back to the All-Hosts Group.

Receiving

At this stage, the scene has been set for multicast data to be received by the browsers that have Real-Time Reporting running. The hosts know who their members are. The All-Hosts Group knows who its hosts are. The routers that service the hosts are aware that their hosts are waiting for multicast data. Symposium Call Center Server now needs to provide that data.

Symposium Call Center Server delivers its real-time statistics data to its IP multicast-capable router on its LAN. The router puts together the data to be sent to the host groups, and maps the address of the multicast All-Hosts Group to the IP address that it uses to send data.

The data is sent from the LAN router to the All-Hosts Group. The All-Hosts Group then sends the data to the routers, whose job it is to receive data for hosts on their network or subnetwork. The routers for each host forward the data to their hosts, and each host forwards the data to its members.

Note: In traveling from the receiver to the sender, the request may travel through several routers. Only the routers nearest to the sender and receiver must be multicast-capable.

Multicast groups and members

Multicast hosts

Any system or router can be a host and can send multicast data to a multicast group if it meets the following conditions:

- The network interface card in the system is multicast-capable.
- The system or router is on a network with a local multicast router.

Note: The sender does not have to be a member of a multicast host group if it is only sending multicast data. Inclusion in a multicast host group is required only if receipt of multicast data is required.

Multicast host groups

Recipients of IP multicasting datagrams are called host groups. Host groups fall into the following two categories:

- permanent host groups
- transient host groups

Permanent host groups are groups with an assigned IP multicast group address. The number of members in the host group is irrelevant in that a permanent host group with no members still exists as long as its IP multicast address is defined.

A transient host group, by contrast, exists only if it has at least one member that requires its services. The multicast IP address for the transient host group is not permanently assigned to the host group; however, the addresses that can be dynamically assigned to a host group have two restrictions. The IP multicast address for a transient host group

- must be in the address range designated for IP multicasting
- cannot be the same as an address for a permanent host group

Multicast groups are virtual groups: they exist only from the point of view of multicast-capable routers or an All-Hosts Group. A host is simply a PC in a network that is designated to accept requests for multicast data from other PCs in the same network. This host conveys its membership status to its designated multicast-capable router. A group is formed when other PCs communicate their desire to join the host's group. The PCs that want to join the group can be from different networks or subnetworks. Their communication with the host makes them part of a single group.

The following groups are some of the permanent host groups that exist in an IP multicast-capable network:

- The All-Hosts Group: This group is used to identify all IP multicast hosts at your organization. When a host reports that it has members who want to receive multicast data, it sends this report to the All-Hosts Group. The multicast IP address for this group is 224.0.0.1.
- The All-Routers Group: This group is used to identify all IP multicast routers at your organization. The multicast IP address for this group is 224.0.0.2.

Multicast host group members

Host group members have few restrictions. They can

- reside anywhere on any network
- join or leave a host group at any time
- join more than one host group

To receive a multicast message

- the member must join the group to which the message is being sent
  and
- the group that the member has joined must belong to a network that is registered with a local multicast router

If the member joins a group that does not belong to a network registered with a local multicast router, the router receives the multicast message but has no way of distributing the message through the network to the member.

Multicast addresses

IP multicasting specifies multicast host groups using Class D Internet Protocol addresses. These host group addresses range from 224.0.0.0 through 239.255.255.255. While IP addresses identify a specific physical location, a multicast IP address identifies a transmission session—a request conveyed from a client to a host to join a multicast group.

However, when choosing IP multicast sending and receiving addresses, you must be aware of the following restrictions:

- The IP multicast addresses between 224.0.0.0 and 224.0.0.255 inclusive are reserved for routing protocols and topology discovery or maintenance protocols.
- Additional IP multicast addresses between 224.0.0.0 and 239.255.255.255 are also reserved for specific applications like Net News.

The IP multicast addresses that you select for IP multicasting groups at your organization *cannot* be within the 224.0.0.0 and 224.0.0.255 range. In addition, you must check to make sure that you do not select an IP multicast address that has already been reserved for a specific multicast application.

The following organizations maintain current information on IP multicasting addressing and can provide access to an extensive list of reserved IP multicast addresses. It is highly recommended that you review the information at one or both of these sites prior to assigning an IP address to a multicast group:

- Internet Engineering Task Force (http://www.ietf.org)
- Internet Assigned Numbers Authority (http://www.iana.org)

Multicast routing methods

The method that multicast routers use to interact with one another depends upon the routing protocol that has been set up for communications. All of these routing protocols use a routing method that moves a multicast packet from its source to its destination(s). There are several different routing methods:

- flooding
- spanning trees
- core-based trees
- reverse path broadcasting
- truncated reverse path broadcasting
- reverse path multicasting

A detailed description of each of these routing methods is beyond the scope of this document. The section below briefly discusses the spanning tree method, one of the more simple and efficient routing methods. To find out more about routing methods, visit the Internet Engineering Task Force (http://www.ietf.org), and Internet Assigned Numbers Authority (http://www.iana.org). Both sites provide additional information and articles that address IP multicast routing methods in greater detail.

Spanning trees

Multicast routing depends upon its multicast-capable routers to exchange information about neighbouring routers and efficiently route multicast traffic. The Internet Group Management Protocol (IGMP) selects one router as the primary router for each physical network in a LAN. This primary router creates a routing method called a spanning tree that connects all other routers that belong to an IP multicast group.

A spanning tree is a loop-free network of paths between routers. Only one path is established between each router. When each router is aware of the branches in the spanning tree, it copies multicast datagrams only to those branches of the tree. With this method, datagrams are duplicated only when the spanning tree branches, keeping the amount of duplication required on a network to a minimum.

Multicast protocols

There are a variety of protocols available for multicast routing. The protocol that your network operations department chooses for your routers depends upon the type of delivery service that you must provide.

If your network configuration does not require the delivery of multicast packets between routers or across networks, you only need the Internet Group Management Protocol. If your multicast data recipients extend beyond a single network, your network operations department must define multicast routing protocols for your routers. These protocols create the spanning trees and forward the multicast packets that are required to get the data to the group members.

The following list includes some of the most common multicast protocols and a brief description of the routing features that each provides.

Internet Group Management Protocol

When clients indicate that they want to join a group, and hosts indicate to routers that they have group members, Internet Group Management Protocol (IGMP) is the protocol used to convey this information between host group members, hosts, and routers. See “How sending and receiving works” on page 561 for more information on how group membership occurs. IGMP must be available on any interface running a multicast protocol, as well as on any static interface over which you want to transfer multicast traffic.

Distance Vector Multicast Routing Protocol

Routers that use Distance Vector Multicast Routing Protocol (DVMRP) advertise the shortest-path routes to the networks on which a multicasting source resides. DVMRP is the opposite of RIP, which advertises routes to destination networks.

Multicasting Extensions to Open Shortest Path First

Routers using Multicasting Extensions to Open Shortest Path First (MOSPF) utilize an enhanced version of Open Shortest Path First (OSPF). This protocol allows a router to forward multicast IP traffic within an autonomous OSPF (v.2) system.

Protocol Independent Multicast

Protocol Independent Multicast (PIM) provides efficient routes for multicast traffic that must cross the Internet to reach members of sparsely distributed multicast groups. The Nortel Networks implementation of PIM supports sparse mode. PIM communicates with far-flung members by

- inviting downstream members to join a shared tree by sending explicit join messages
- using rendezvous points (RPs) for receivers to meet new sources. Sources announce their existence to RPs; receivers query RPs to learn about multicast sessions.
- establishing a shortest-path tree to create a data path between sources and receivers

Resource Reservation Protocol

Resource Reservation Protocol (RSVP)-capable routers allow their host systems in an IP network to reserve resources for unicast or multicast dataflows.

Packet migration between multicast and non-multicast networks

With the variety of networks that exist and the data that must travel between them, it is too expensive and difficult (if not impossible) to set up network infrastructures that carry only multicast packets, while unicast networks carry only unicast data. The implementation of multicasting in your network does not preclude the transmission of unicast packets.

You can configure your routers to allow tunneling — unicast packets that travel as multicast packets, and multicast packets that travel as unicast packages between multicast and non-multicast networks. The table below provides an overview of how different packet types can travel between multicast and non-multicast networks:

Router receives	On interface type	Forwarding Action and How to Enable
Unicast or broadcast packet	Multicast	The multicast protocol running on the interface forwards the packet to a multicast destination address (or list of multicast destination addresses) dictated by an IP traffic filter. The IP traffic filter must be configured to convert the unicast or broadcast packets to multicast.
Multicast	Multicast	The router's multicast protocol forwards the packet to ■ a multicast configured outbound interface (based on multicast protocol decisions) or ■ a non-multicast, IGMP static configured outbound circuit In Site Manager, you must set the IGMP static forwarding entries policy for Dynamic to Static forwarding mode.

Router receives	On interface type	Forwarding Action and How to Enable
Multicast	Non-multicast, IGMP static configured	The router forwards multicast packet traffic to a multicast enabled network if ■ multicast protocols are running on the routers ■ the IGMP static forwarding policy is set to Static to Dynamic ■ the IGMP interface parameter Static Forward Cache Lifetime is set to a value in accordance with the multicast protocol (DVMRP or MOSPF) running on the router
Multicast	Non-multicast, IGMP static configured	The router forwards the multicast traffic to a non-multicast, static configured interface if ■ the IGMP static forwarding policy is set to Static mode

Implementing IP multicasting for Symposium Web Client

IP multicast requirements

The preceding sections discussed how multicasting works, the communication between software and hardware that multicasting generates, and the routing and related protocols that make the transmission of multicast data between sources and destinations possible. With this information, you can begin considering how to implement IP multicasting for your specific LAN or WAN, or both, to facilitate Symposium Web Client's real-time data multicasting requirements.

The following list is a checklist of the requirements that must apply to your network, network components, and multicast-capable applications for Symposium Web Client's multicasting capabilities to work in a simple LAN configuration:

Requirements for multicast communication on one LAN	
The sending and receiving nodes in your network must be multicast-enabled.	
The TCP/IP protocol stack must support IP multicast sending and receiving.	
The software used to communicate a request to join a multicast group must support the IGMP protocol.	
IGMP must be configured on all routers that receive or forward multicast or non-multicast datagrams.	

Requirements for multicast communication on one LAN	
The network interface cards and their drivers at the sending and receiving nodes must be able to filter for LAN data link layer addresses that have been mapped from network layer IP multicast addresses. **Note:** If there are two network interface cards installed on the application server (one for the ELAN and the other for the CLAN), then you must manually configure the cards so the application server always sends multicast data through the CLAN card. The client PCs are located on the CLAN and, therefore, expect to receive multicast data on this network. For more information, see “The send address on the application server is the point from which multicast data is sent to the clients. The multicast-enabled router acts as both the host and the All-Hosts Group to the clients who become host group members when they open a browser and launch Real-Time Reporting.” on page 574.	
IP multicasting software must be installed on clients that need to receive multicast data.	

Routers are not required for a host to join a multicast group and share multicast data with other hosts on the same subnetwork. When multicast sending and receiving must travel between WANs and LANs, the list of requirements includes the above checklist in addition to the items below:

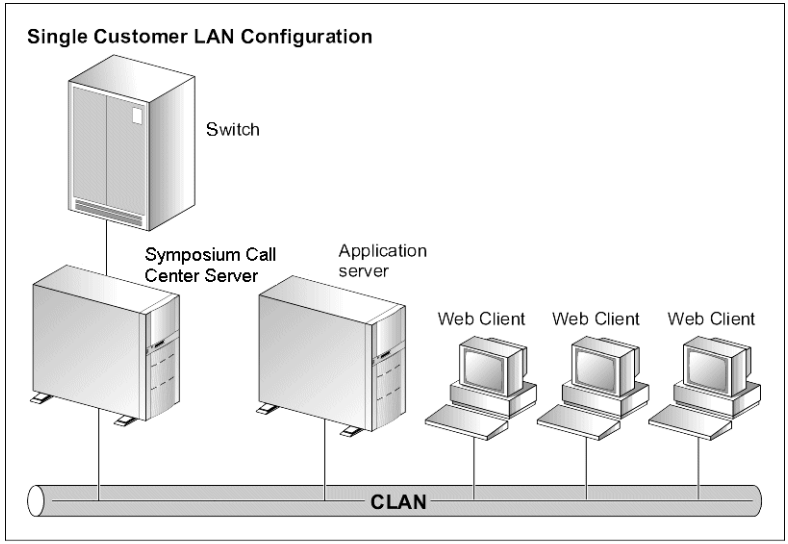
Requirements for multiple LANs or LAN-to-WAN multicast communication	
Intermediate routers between sending and receiving nodes must be IP multicast-capable.	
Firewalls between LANs and WANs must be configured to permit IP multicast traffic.	
An IP traffic filter must be able to convert packets from unicast to broadcast or broadcast to unicast.	
An IP traffic filter must be able to convert packets from unicast to multicast or multicast to unicast.	

Requirements for multiple LANs or LAN-to-WAN multicast communication	
Configure an IGMP static forwarding policy for interfaces that multicast and for interfaces that do not multicast.	
Set policy filters to identify multicast protocol-compliant gateways, interfaces, tunnels, and networks for IGMP, DVMRP, and MOSPF.	
Configure the network interface cards on the application server so it always sends multicast data through the CLAN card. For more information, see “The send address on the application server is the point from which multicast data is sent to the clients. The multicast-enabled router acts as both the host and the All-Hosts Group to the clients who become host group members when they open a browser and launch Real-Time Reporting.” on page 574.	

Network deployment scenarios

Single LAN

In a single LAN environment, the clients, the application server, and Symposium Call Center Server share a LAN. With no firewalls to potentially block access, this is the simplest environment to configure for IP multicasting.



When Symposium Web Client is installed, its IP multicast send and receive addresses are identified on the application server. Symposium Web Client uses the receive address to collect multicast data from Symposium Call Center Server. The IP multicast receive address on Symposium Web Client must be the same as the IP multicast send address of the server in Symposium Call Center Server. However, the IP multicast receive address on Symposium Web Client must be different from the IP multicast send address on Symposium Web Client.

The send address on the application server is the point from which multicast data is sent to the clients. The multicast-enabled router acts as both the host and the All-Hosts Group to the clients who become host group members when they open a browser and launch Real-Time Reporting.

Appendix C

Web site types

In this appendix

Determining your web site type 576

Determining your web site type

Introduction

To determine which web site type is best for your organization when you install Symposium Web Client, evaluate how you intend to use the application server on which Symposium Web Client will reside.

Web sites and virtual directories

There are two ways in which you can install Symposium Web Client on the application server:

- as a stand-alone Symposium Web Client web site
- as a "sub-site" or virtual directory attached to an existing web site

Note: You must specify the type of web site that Symposium Web Client uses in step 13 of the Symposium Web Client installation process. For more information, see "To install Symposium Web Client on the application server" on page 98.

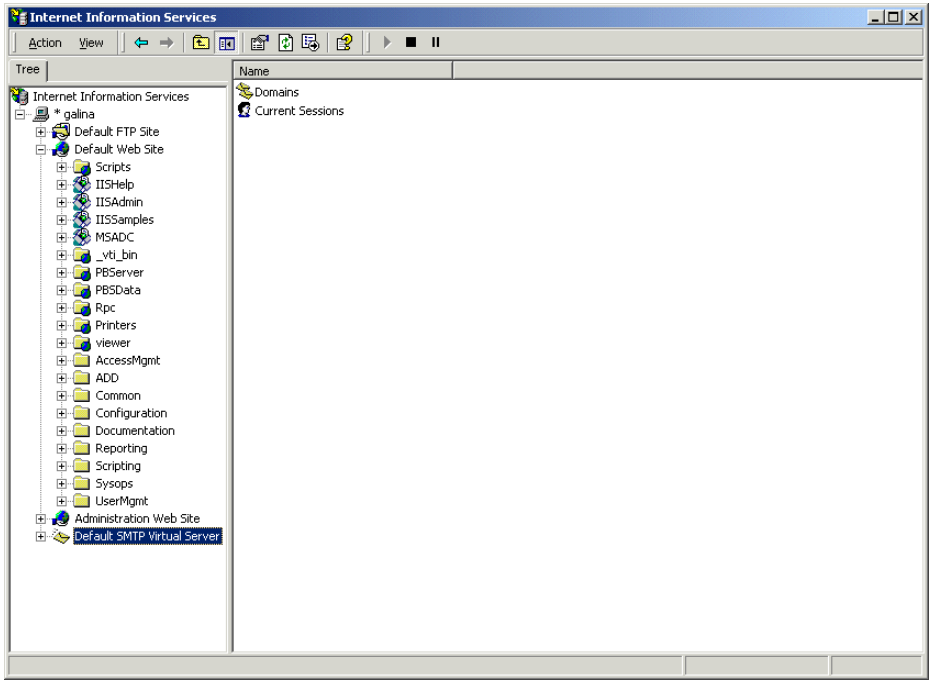
Regardless of the type of web site that you choose, the application behaves in the same way, and is visible to client PCs in the same way. The only significant difference between a virtual directory web site and a default web site is the way in which it appears in Windows 2000 Server.

Symposium Web Client as a stand-alone web site

If Symposium Web Client fits the following criteria, you should set up Web Client as the default web site:

- Symposium Web Client is the only application that will run on the application server.
- The existing company intranet or extranet is on another server, entirely separate from the domain being used for Web Client.

When Symposium Web Client is installed as a default web site, it appears as follows:

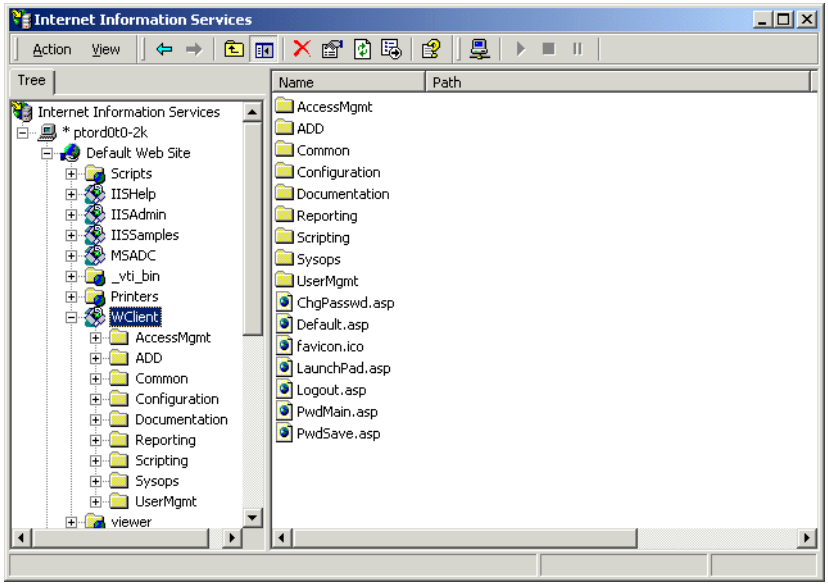


Symposium Web Client as a virtual directory

Set up Symposium Web Client as a virtual directory on an existing web site if Symposium Web Client fits the following criteria:

- You have a company intranet or extranet, or both, that already resides on the application server.
- You are installing Symposium Web Client as an additional web site on the application server.

When Symposium Web Client is installed as a virtual directory, it appears as a folder called WClient in the Default Web Site tree.



Appendix D

Third-party controls required on the client PC

In this appendix

Third-party controls 580

Third-party controls

Introduction

The following table lists the third-party controls that are required on the client PC, along with the names of the files, and the version number required for Symposium Web Client 4.5. Third-party client controls are required for all Symposium Web Client 4.5 components except Configuration and Audit Trail. For more information on installing third-party controls, see “Installing third-party controls on a client” on page 309.

Control	CAB file	Control File	Company	Purpose	Version
Crystal Reports Viewer	activexviewermod.cab	crviewer9.dll	Crystal Decisions	Crystal Reports	9.2.0.720
Emergency Help	EHCtrl.cab	iceemhlpcontrol.dll	Nortel Networks	Emergency Help	4.5.2.0
Popup Menu	iemenu.cab	iemenu.ocx	Microsoft	Internet Explorer Popup Menu	4.71.115.0
Date and Time Picker	MSCOMCT2.cab	mscomct2.ocx	Microsoft	Time and date picker control	6.0.88.4
Remote Desktop Client	msrdp.cab	msrdp.ocx	Microsoft	Terminal Services	5.1.2600.1095
Olectra Chart	olec-2D.cab	olch2x32.ocx	ComponentOne	Chart control	6.0.15.0
Real-time Display	RtdCtrl.cab	icertdcontrol.dll	Nortel Networks	Real-time displays	4.5.0.5
Sheridan ActiveTreeView	ssTree.cab	SSTree.ocx	Infragistics	TreeView control	1.0.2.8
True OLE DB Grid 6	todg6.cab	todg6.ocx	Apex Software	Grid control	6.0.0.235
Windows Scripting Shell None*	Windows OS	whsom.ocx	Microsoft	Reads from the registry	Depends on the client OS

Control	CAB file	Control File	Company	Purpose	Version
SOAP Client 3.0*	SOAP install	MSSOAP30.dll	Microsoft	Access to server-side functionality	3.0.1325.0

*Unlike the other controls listed in the table, these two controls are not downloaded to the client PC, but they are required for proper Symposium Web Client functionality. For more information on installing the client version of SOAP, see “Installing Simple Object Access Protocol” on page 305. The control for Windows scripting is automatically installed with the client operating system.

Appendix E

Supervisor/reporting agents matrix

In this appendix

Overview 584

Real-Time Reporting 585

Historical Reporting 591

Contact Center Management 593

Overview

Introduction

The supervisor/reporting agents feature enables you to dynamically link a supervisor and all his or her reporting agents with one or more Web Client users, thereby enabling the users to view the agents in Symposium Web Client components, such as Real-Time and Historical Reporting, and Contact Center Management. You assign supervisor/reporting agent combinations to Web Client users by using the **Supervisors** tab in the User Properties window of Access and Partition Management.

Supervisor/reporting agent combinations and partitions affect the data that users see differently, based on the component in which the user is working and the type of data the user is viewing (for example, a private real-time display behaves differently than a public real-time display). The tables in this appendix outline the effect of supervisor/reporting agent combinations and partitions in each of the applicable Symposium Web Client components.

In most cases, the supervisor/reporting agents feature only works in conjunction with partitions; you must assign both a partition and a supervisor/reporting combination to a user to restrict the user to seeing his or her reporting agents. The exception to this rule is in Real-Time Reporting, and specifically for the private agent real-time displays and agent map displays. If you have assigned the user *only* a supervisor/reporting agent combination in Access and Partition Management (not a partition), then the user can apply this supervisor/reporting agent combination (on the Filters tab) to either a private agent real-time display, or an agent map display to view only those reporting agents.

Real-Time Reporting

Introduction

The data that users see in Real-Time Reporting varies based on whether the user opens a *public* agent real-time display, a *private* agent real-time display, or an agent map display. These differences are summarized in the following tables:

Public agent real-time displays

Has an administrator assigned the user a partition in Access and Partition Management?	Has the user assigned a custom filter to the display?	Has an administrator assigned the user a supervisor/ reporting agent combination in Access and Partition Management?	Data the user sees in the display
Yes	N/A*	No*	Only agents included in the partition
Yes	N/A	Yes	Only agents included in the partition
No	N/A	No	All agents
No	N/A	Yes	All agents
Yes (no agents)	N/A	No	No data

Has an administrator assigned the user a partition in Access and Partition Management?	Has the user assigned a custom filter to the display?	Has an administrator assigned the user a supervisor/ reporting agent combination in Access and Partition Management?	Data the user sees in the display
Yes (no agents)	N/A	Yes	No data
Yes (no agents)	N/A	Yes (but the supervisor has no reporting agents)	No data
Yes	N/A	Yes (but the supervisor has no reporting agents)	Only agents included in the partition
No	N/A	Yes (but the supervisor has no reporting agents)	All agents

*Users cannot apply custom filters or supervisor/reporting agent combinations to public real-time displays. If you assign the user a supervisor/reporting agent combination in Access and Partition Management, it does *not* affect the data that the user sees in public agent real-time displays, regardless of whether the user has a partition assigned to him or her. Only partitions affect the data that users see in public agent real-time displays.

Private agent real-time displays

Unlike public agent real-time displays, for private real-time displays, users can create custom filters by choosing the items from their partitioned data that they want to see in the display. Then, when they are customizing their private display, they can assign one or more of these filters to the display in the Filters tab.

This tab also lists any supervisor/reporting agent combinations that the administrator has assigned to the user in Access and Partition Management, represented by the corresponding supervisor's name. Each supervisor name represents all of that supervisor's reporting agents.

Based on the supervisor/reporting agent combinations that the administrator has assigned to the user, there may be more than one supervisor name on this tab. For example, the administrator can assign the supervisor his or her own agents (and, therefore, the supervisor's own name appears on this tab), and the reporting agents of another supervisor, in which case this other supervisor's name appears on the tab too. When the user customizes the display, he or she can assign the supervisor/reporting agent combinations to the display by clicking the names of the appropriate supervisors to view all the reporting agents of these selected supervisors.

Note: Private real-time displays are different than public real-time displays in that users do not require a partition to restrict the agent data that they can see in the display. If the administrator assigns the user *only* a supervisor/reporting agent combination in Access and Partition Management (not a partition), then the user can apply this supervisor/reporting agent combination (on the Filters tab) to the private agent real-time display to view only those reporting agents.

Has an administrator assigned the user a partition in Access and Partition Management?	**Has the user assigned a custom filter to the display?**	**Has the user assigned a supervisor/ reporting agent combination to the display?**	**Data the user sees in the display**
Yes	Yes	No	Only the agents included in the custom filter
Yes	No	No	Only the agents included in the partition
Yes	Yes	Yes	All agents in the custom filter, plus the agents reporting to the selected supervisor

Has an administrator assigned the user a partition in Access and Partition Management?	Has the user assigned a custom filter to the display?	Has the user assigned a supervisor/ reporting agent combination to the display?	Data the user sees in the display
Yes	No	Yes	Only the agents reporting to the selected supervisor
No	No	No	All agents
No	No	Yes	Only the agents reporting to the selected supervisor
Yes (no agents)	No	No	No data
Yes (no agents)	No	Yes	Only the agents reporting to the selected supervisor
Yes	Yes	Yes (but the supervisor has no reporting agents)	Only the agents included in the custom filter
Yes	No	Yes (but the supervisor has no reporting agents)	No data
Yes (no agents)	No	Yes (but the supervisor has no reporting agents)	No data
No	No	Yes (but the supervisor has no reporting agents)	No data

Agent map graphical displays

Before a user can launch an agent map graphical display, he or she must apply either a custom filter to it, or a supervisor/reporting agent combination, but the user cannot apply both at the same time.

Note: Agent map graphical displays are different than public real-time displays in that users do not require a partition to restrict the agent data that they can see in the display. If the administrator assigns the user *only* a supervisor/reporting agent combination in Access and Partition Management (not a partition), then the user can apply this supervisor/reporting agent combination to the agent map display to view only those reporting agents.

Has an administrator assigned the user a partition in Access and Partition Management?	Has the user assigned a custom filter to the display?	Has the user assigned a supervisor/reporting agent combination to the display?	Data the user sees in the display
Yes	Yes	No	Only agents included in the custom filter
Yes	No	Yes	Only the agents reporting to the selected supervisor
No	No	Yes	Only the agents reporting to the selected supervisor
Yes (no agents)	No	Yes	Only the agents reporting to the selected supervisor
Yes (no agents)	No	Yes (but the supervisor has no reporting agents)	No data
No	No	Yes (but the supervisor has no reporting agents)	No data

Has an administrator assigned the user a partition in Access and Partition Management?	Has the user assigned a custom filter to the display?	Has the user assigned a supervisor/reporting agent combination to the display?	Data the user sees in the display
Yes	No	Yes (but the supervisor has no reporting agents)	No data

Historical Reporting

Introduction

In Historical Reporting, if users do not have a partition assigned to them, then they see all agent data in the selection criteria, regardless of whether they have a supervisor/reporting agent combination assigned to their user profile.

In this component, partitions and supervisor/reporting agent combinations affect the data that users see in the Selection Criteria box. The selection criteria feature in Historical Reporting is like the filters feature in Real-Time Reporting.

Just as Real-Time Reporting users can choose the data they want to see in the displays by creating custom filters and assigning them to the displays, so too can Historical Reporting users specify which items from their partitioned data they want to see in the historical reports by choosing from the selection criteria. If users have not been assigned a partition, then they can choose from all data.

Has an administrator assigned the user a partition in Access and Partition Management?	Has an administrator assigned the user a supervisor/reporting agent combination in Access and Partition Management?	What data is available for the user to choose from in the selection criteria?	Data the user sees in the report
Yes	No	All agents in the partition	The agents the user has chosen from the selection criteria
No	No	All agents	The agents the user has chosen from the selection criteria
Yes	Yes	The agents in the partition and the agents included in the supervisor/ reporting agent combination assigned to this user	The agents the user has chosen from the selection criteria

Has an administrator assigned the user a partition in Access and Partition Management?	Has an administrator assigned the user a supervisor/reporting agent combination in Access and Partition Management?	What data is available for the user to choose from in the selection criteria?	Data the user sees in the report
No	Yes	All agents	The agents the user has chosen from the selection criteria
Yes (no agents)	No	No data	No data
Yes (no agents)	Yes	The agents included in the supervisor/ reporting agent combination assigned to this user	The agents the user has chosen from the selection criteria
Yes (no agents)	Yes (but the supervisor has no reporting agents)	No data	No data
Yes	Yes (but the supervisor has no reporting agents)	All agents in the partition	The agents the user has chosen from the selection criteria
No	Yes (but the supervisor has no reporting agents)	All agents	The agents the user has chosen from the selection criteria

Contact Center Management

Introduction

In Contact Center Management, if users do not have a partition assigned to them, then they see all agent data, regardless of whether they have a supervisor/ reporting agent combination assigned to their user profile.

Note: The administrator can also control the data users see in Contact Center Management by assigning access classes to them. Access classes can restrict the windows or portions of windows that users can open in the application, and the actions users can perform. In addition, if the administrator assigns users the *Use Agent & Skillset Partitions in CCM* access class, then they are restricted to viewing only their partitioned skillsets (in addition to their partitioned agents, which is the default behavior).

Has an administrator assigned the user a partition in Access and Partition Management?	Has an administrator assigned the user a supervisor/reporting agent combination in Access and Partition Management?	Data the user sees in Contact Center Management
Yes	No	Only the agents in the partition
Yes	Yes	The agents in the partition and the agents included in the supervisor/reporting agent combination assigned to this user
No	No	All agents
No	Yes	All agents
Yes (no agents)	Yes	The agents included in the supervisor/reporting agent combination assigned to this user

Has an administrator assigned the user a partition in Access and Partition Management?	Has an administrator assigned the user a supervisor/reporting agent combination in Access and Partition Management?	Data the user sees in Contact Center Management
Yes (no agents)	No	No agents
Yes (no agents)	Yes (but the supervisor has no reporting agents)	No agents
Yes	Yes (but the supervisor has no reporting agents)	The agents in the partition
No	Yes (but the supervisor has no reporting agents)	All agents

Glossary

A

accelerator key

A key on a phoneset that an agent can use to place a call quickly. When an agent presses an accelerator key, the system places the call to the configured number associated with the key. For example, if an agent presses the Emergency key, the system places a call to the agent's supervisor.

access class

A collection of access levels that defines the actions a member of the access class can perform within the system. For example, a member of the Administrator access class might be given a collection of Read/Write access levels.

access level

A level of access or permission given to a particular user for a particular application or function. For example, a user might be given View Only access to historical reports.

ACCESS link

A communication channel between Symposium Call Center Server and CallPilot or Meridian Mail.

ACCESS voice port

A voice port that is controlled by the ACCESS link.

ACD call

See Automatic call distribution call.

ACD-DN

See Automatic call distribution directory number.

ACD group

See Automatic call distribution group.

ACD routing table
See Automatic call distribution routing table.

ACD subgroup
See Automatic call distribution subgroup.

acquired resource
A resource configured on the switch that is under the control of Symposium Call Center Server. Resources must be configured with matching values on both the switch and Symposium Call Center Server.

activated script
A script that is processing calls or is ready to process calls. Before you can activate a script, you must first validate it.

activity code
A number that an agent enters on his or her phoneset during a call. Activity codes provide a way of tracking the time agents spend on various types of incoming calls. They are also known as Line of Business (LOB) codes. For example, the activity code 720 might be used to track sales calls. Agents can then enter 720 on their phonesets during sales calls, and this information can be generated in an Activity Code report.

adapter
Hardware required to support a particular device. For example, network adapters provide a port for the network wire. Adapters can be expansion boards or part of the computer’s main circuitry.

ADD
Agent Desktop Displays

administrator
A user who is responsible for setting up and maintaining Symposium Web Client.

agent
A user who is responsible for handling customer calls.

agent login ID

A unique identification number assigned to a particular agent. The agent uses this number when logging on. The agent ID is not associated with any particular phoneset.

agent to skillset assignment

A matrix that, when you run it, sets the priority of one or more agents for a skillset. Agent to skillset assignments can be scheduled.

agent to supervisor assignment

A definition that, when you run it, assigns one or more agents to specific supervisors. Agent to supervisor assignments can be scheduled.

AIP

Advanced I/O Processor

API

See application program interface

application

1. A logical entity that represents a Symposium Web Client script for reporting purposes. The Master script and each primary script have an associated application. The application has the same name as the script it represents.
2. A program that runs on a computer.

application program interface

A set of routines, protocols, and tools that programmers use to develop software applications. APIs simplify the development process by providing commonly used programming procedures.

application server

The computer hosting the web server that distributes all the web pages to the client PCs that are using Symposium Web Client. The client PCs use an Internet browser interface to connect to the application server, launch Symposium Web Client, and interact with Symposium Call Center Server. The application software for Symposium Web Client is installed on the application server.

associated supervisor

A supervisor who is available for an agent if the agent's reporting supervisor is unavailable. *See also* reporting supervisor.

Automatic call distribution

A means of automatically distributing an organization's incoming calls among a number of answering positions (ACD agents). Automatic call distribution is useful in operations where callers want a service rather than a specific person. Calls are serviced in the order they arrive and are distributed so that the workload at each answering position is approximately equal.

Automatic call distribution call

A call to an ACD-DN. ACD calls are distributed to agents in an ACD group based on the ACD routing table on the switch. *See also* Automatic call distribution directory number.

Automatic call distribution directory number

A primary or supplementary DN associated with an ACD group. Calls made to an automatic call distribution directory number are distributed to agents belonging to the group, based on the ACD routing table on the switch.

Automatic call distribution group

An entity defined on the switch for the purpose of call distribution. When a customer dials an ACD group, the call is routed to any agent who is a member of that group.

Automatic call distribution routing table

A table configured on the switch that contains a list of ACD-DNs used to define routes for incoming calls. This ensures that incoming calls not processed by Symposium Call Center Server will be queued to ACD groups and handled by available agents.

Automatic call distribution subgroup

An entity defined on the switch to assign supervisory responsibilities. Each subgroup has one supervisor phoneset and a number of agent phonesets associated with it. Agents can log on to any phoneset within their ACD subgroup. The supervisor must log on to the supervisor phoneset to monitor his or her assigned agents.

C

call age
The amount of time a call was waiting in the system before being answered by an agent.

call destination
The site to which an outgoing network call is sent. *See also* call source.

call intrinsic
A script element that stores call-related information assigned when a call enters Symposium Call Center Server. *See also* intrinsic, skillset intrinsic, time intrinsic, and traffic intrinsic.

CallPilot
A multimedia messaging system you can use to manage many types of information, including voice messages, fax messages, e-mail messages, telephone calls (including conferencing), calendars, and directories.

call presentation class
A collection of preferences that determines how calls are presented to an agent**.** A call presentation class specifies whether a break time between calls is allowed, whether an agent can put DN calls on hold for incoming ACD calls, and whether an agent phoneset displays that the agent is reserved for a network call.

call priority
A numerical value assigned in a script that defines the relative importance of a call. If two calls are in the queue when an agent becomes available, and one call is queued with a higher priority than the other, the agent receives the higher priority call first. *See also* skillset priority.

call source
The site from which an incoming network call originates. *See also* call destination.

call treatment
A script element that enables you to provide handling to a call while it is waiting to be answered by a call center agent. For example, a caller can hear a recorded announcement or music while waiting for an agent.

call variable

A script variable that applies to a specific call. A call variable follows the call through the system and is passed from one script to another with the call. *See also* global variable, script variable.

Calling Line Identification

An optional service that identifies the telephone number of the caller. This information can then be used to route the call to the appropriate agent or skillset. The CLID can also be displayed on an agent's phoneset.

CCM

Contact Center Management

CDN

See controlled directory number.

CLAN

See Customer local area network.

CLID

See Calling Line Identification.

client

The part of Symposium Call Center Server that runs on a personal computer or workstation and relies on the server to perform some operations. *See also* server.

command

A building block used with expressions, variables, and intrinsics to create scripts. Commands perform distinct functions, such as routing a call to a specific destination, playing music to a caller, or disconnecting a caller.

controlled directory number

A special directory number that allows calls arriving at the switch to be queued when the CDN is controlled by an application such as Symposium Call Center Server. When a call arrives at this number, the switch notifies the application and waits for routing instructions, which are performed by scripts in Symposium Call Center Server.

CSE 1000 switch
Succession Communication Server for Enterprise 1000 switch

Customer local area network
The LAN to which your corporate services and resources connect. The Symposium Web Client application server and client PC both connect to the CLAN. Third-party applications that interface with the server also connect to this LAN.

D

DBMS
Database Management System

deactivated script
A script that does not process any new calls. If a script is in use when it is deactivated, calls continue to be processed by the script until they are completed.

default activity code
The activity code that is assigned to a call if an agent does not enter an activity code manually, or when an agent presses the activity code button twice on his or her phoneset.

Each skillset has a defined default activity code.

default skillset
The skillset to which calls are queued if they have not been queued to a skillset or a specific agent by the end of a script.

destination site
The site to which an outgoing network call is sent. *See also* source site.

DHCP
See dynamic host configuration protocol.

Dial-Up Networking
See Remote Access Services.

Dialed Number Identification Service

An optional service that allows Symposium Call Center Server to identify the phone number dialed by the incoming caller. An agent can receive calls from customers calling in on different DNISs and, if the DNIS is displayed on the phoneset, can prepare a response according to the DNIS.

Digital Multiplex Switch

A Nortel Networks switch for the central office market.

directory number

The number that identifies a phoneset on a switch. The directory number (DN) can be a local extension (local DN), a public network telephone number, or an automatic call distribution directory number (ACD-DN).

directory number call

A call that is presented to the DN key on an agent's phoneset.

display threshold

A threshold used in real-time displays to highlight a value below or above the normal range.

DMS

See Digital Multiplex Switch.

DN

See directory number.

DN call

See directory number call.

DNIS

See Dialed Number Identification Service.

DNS

See Domain Name System.

domain

A domain represents the portion of a network on which a common security policy applies. A domain's security policy defines the characteristics of passwords, user accounts, and so on.

Domain Name System

The protocols and services on a TCP/IP network that allow network users to use the name of a computer, rather than an IP address, when looking for other computers.

dongle

The attachment plugged into the parallel port of a server connected to a DMS/MSL-100 switch that authenticates the serial number required at the time of server installation.

dynamic host configuration protocol

A protocol for dynamically assigning IP addresses to devices on a network.

dynamic link library

A library of executable functions or data that can be used by a Windows application. Typically, a DLL provides one or more particular functions and a program accesses the functions by creating either a static or dynamic link to the DLL. Several applications can use a DLL at the same time.

E

ELAN

See embedded local area network.

embedded local area network

A dedicated Ethernet TCP/IP LAN that connects the server in Symposium Call Center Server and the switch.

Emergency key

A key on an agent's phoneset that, when pressed by an agent, automatically calls his or her supervisor to notify the supervisor of a problem with a caller.

event

1. An occurrence or action in Symposium Web Client, such as the sending or receiving of a message, the opening or closing of an application, or the reporting of an error. Some events are for information only, while others can indicate a problem. Events are categorized by severity: information, minor, major, and critical. 2. An action generated by a script command, such as queuing a call to a skillset or playing music.

expression

A building block used in scripts to test for conditions, perform calculations, or compare values within scripts. *See also* logical expression, mathematical expression, and relational expression.

F

filter

1. In Real-Time Reporting, you create filters by specifying the skillset, application, and agent data that you want to see in the real-time displays. You can apply as many filters as you want to each display. After you apply these filters to the real-time displays, you no longer have to scan data that is not applicable to you. 2. In Historical Reporting, you can select the elements that you want to include in your reports by choosing filters and assigning filter elements to your reports. For example, in an agent performance report, you can choose the filter Agent Login ID, and then choose the filter elements (the logon IDs) that you want to report on.

filter timer

The length of time after the system unsuccessfully attempts to route calls to a destination site, before that site is filtered out of a routing table.

first-level threshold

The value that represents the lowest value of the normal range for a statistic in a threshold class. The system tracks how often the value for the statistic falls below this value.

G

global settings

Settings that apply to all skillsets or IVR ACD-DNs that are configured on your system.

global variable

A variable that contains values that can be used by any script on the system. You can only change the value of a global variable in the Script Variable Properties sheet. You cannot change it in a script. *See also* call variable, variable.

I

IIS

See Internet Information Services.

Interactive voice response

An application that allows telephone callers to interact with a host computer using prerecorded messages and prompts.

Interactive voice response ACD-DN

A directory number that routes a caller to a specific IVR application. An IVR ACD-DN must be acquired for non-integrated IVR systems.

Interactive voice response event

A voice port logon or logoff. An IVR event is pegged in the database when a call acquires or de-acquires a voice port.

Internet Information Services

Microsoft's Web server software. IIS uses Hypertext Transfer Protocol (HTTP) to provide World Wide Web documents in a browser. IIS includes several security functions and allows the use of Gopher and File Transfer Protocol (FTP) servers.

Internet Protocol address

An identifier for a computer or device on a TCP/IP network. Networks use the TCP/IP protocol to route messages based on the IP address of the destination. For customers using NSBR, site IP addresses must be unique and correct. The format of an IP address is a 32-bit numeric address written as four values separated by periods. Each value can be 0 to 255. For example, 1.160.10.240 could be an IP address.

intrinsic
A word or phrase used in a script to gain access to system information about skillsets, agents, time, and call traffic that can then be used in formulas and decision-making statements. *See also* call intrinsic, skillset intrinsic, time intrinsic, and traffic intrinsic.

IP address
See Internet Protocol address.

IVR
See Interactive voice response.

IVR ACD-DN
See Interactive voice response ACD-DN.

IVR event
See Interactive voice response event.

IVR port
See voice port.

L

LAN
See Local area network.

Line of Business code
See activity code.

LOB code
See activity code.

Local area network
A computer network that spans a relatively small area. Most LANs connect workstations and personal computers and are confined to a single building or group of buildings.

local call
A call that originates at the local site. *See also* network call.

local skillset

A skillset that can be used at the local site only. *See also* network skillset, skillset.

logical expression

A symbol used in scripts to test for different conditions. Logical expressions are AND, OR, and NOT. *See also* expression, mathematical expression, and relational expression.

M

M1

Meridian 1 switch

M1 IE

Meridian 1 Internet Enabled switch

Management Information Base

A data structure that describes the collection of all possible objects in a network. Each managed node maintains one or more variables (objects) that describe its state. Symposium Call Center Server Management Information Bases (MIBs) contribute to the overall network MIB by

- identifying Nortel Networks/Meridian/Symposium Call Center Server nodes within the network
- identifying significant events (SNMP traps), such as alarms reporting
- specifying formats of alarms

Master script

The first script executed when a call arrives at Symposium Call Center Server. A default Master script is provided with Symposium Web Client, but it can be customized by an authorized user. It can be deactivated but not deleted. *See also* network script, primary script, script, secondary script.

mathematical expression

An expression used in scripts to add, subtract, multiply, and divide values. Mathematical expressions are addition (+), subtraction (-), division (/), and multiplication (*). *See also* expression, logical expression, and relational expression.

Meridian Link Services
A communications facility that provides an interface between the switch and a third-party host application.

Meridian Mail
A Nortel Networks product that provides voice messaging and other voice and fax services.

Meridian MAX
A Nortel Networks product that provides call processing based on ACD routing.

MIB
See Management Information Base.

MLS
See Meridian Link Services.

MM
See Meridian Mail.

MSL-100
Meridian Stored Logic 100 switch

music route
A resource installed on the switch that provides music to callers while they wait for an agent.

N

NACD call
A call that arrives at the server from a network ACD-DN.

NCC
See Network Control Center.

NCRTD
Network Consolidated Real-Time Displays

network call

A call that originates at another site in the network. *See also* local call.

Network Control Center

The server in a Symposium Call Center Server system where NSBR is configured and where communication between servers is managed.

network call

A call that originates at another site in the network. *See also* local call.

network interface card

An expansion board that enables a PC to be connected to a local area network (LAN).

network script

The script that is executed to handle error conditions for Symposium Call Center Server calls forwarded from one site to another, for customers using NSBR. The network script is a system-defined script provided with Symposium Web Client, but it can be customized by an authorized user. It can be deactivated but not deleted. *See also* Master script, primary script, script, secondary script.

Network Skill-Based Routing

An optional feature with Symposium Call Center Server that provides skill-based routing to multiple networked sites.

network skillset

A skillset that is common to every site on the network. Network skillsets must be created at the Network Control Center (NCC).

night mode

A skillset state in which the server does not queue incoming calls to the skillset, and in which all queued calls are given night treatment. A skillset goes into night mode automatically when the last agent logs off, or the administrator can put it into night mode manually. *See also* out-of-service mode, transition mode.

NPA

See Number Plan Area.

NSBR
See Network Skill-Based Routing.

Number Plan Area
Area code

O

object linking and embedding
A compound document standard that enables you to create objects with one application and then link or embed them in a second application.

ODBC
See Open Database Connectivity.

OEM
Original equipment manufacturer

OLE
See object linking and embedding.

Open Database Connectivity
A Microsoft-defined database application program interface (API) standard.

out-of-service mode
A skillset state in which the skillset does not take calls. A skillset is out of service if there are no agents logged on or if the supervisor puts the skillset into out-of-service mode manually. *See also* night mode, transition mode.

out-of-service skillset
A skillset that is not taking any new calls. While a skillset is out of service, incoming calls cannot be queued to the skillset. *See also* local skillset, network skillset, skillset.

P

partition
Partitions enable call center administrators to control the data that Symposium Web Client users can view and manage in Historical Reporting, Real-Time Reporting, and Contact Center Management. Partitions can contain six types of data: agents, skillsets, applications, CDNs, DNISs, and report groups. If an administrator does not assign a partition to a user, then the user sees all available data in the real-time displays and historical reports. However, if the administrator does not assign a partition to a supervisor containing agents, then the supervisor sees nothing in Contact Center Management.

PBX
See private branch exchange.

pegging
The action of incrementing statistical counters to track and report on system events.

pegging threshold
A threshold used to define a cut-off value for statistics, such as short call and service level. Pegging thresholds are used in reports.

PEP
See Performance Enhancement Package.

Performance Enhancement Package
A Symposium Call Center Server supplementary software application that enhances the functionality of previously released software by improving performance, adding functionality, or correcting a problem discovered since the original release.

personal directory number
A DN on which an agent can be reached directly, usually for private calls.

phoneset
The physical device, connected to the switch, to which calls are presented. Each agent and supervisor must have a phoneset.

phoneset display
The display area on an agent's phoneset where information about incoming calls can be communicated.

Position ID
A unique identifier for a phoneset, used by the switch to route calls to the phoneset. Referred to as Telephony/Port Address in Symposium Call Center Server.

primary ACD-DN
A directory number that callers can dial to reach an ACD group.

primary script
A script that is executed or referenced by the Master script. A primary script can route calls to skillsets, or it can transfer routing control to a secondary script. *See also* Master script, network script, script, secondary script.

private branch exchange
A telephone switch, typically used by a business to service its internal telephone needs. A PBX usually offers more advanced features than are generally available on the public network.

R

RAID
See Redundant Array of Intelligent/Inexpensive Disks.

RAN
recorded announcement

RAN route
See recorded announcement route.

RAS
See Remote Access Services.

recorded announcement route
A resource installed on the switch that offers a recorded announcement to callers.

Redundant Array of Intelligent/Inexpensive Disks

A category of disk drives that employs two or more drives in combination for fault tolerance and performance.

relational expression

An expression used in scripts to test for different conditions. Relational expressions are less than (<), greater than (>), less than or equal to (< =), greater than or equal to (> =), and not equal to (< >). *See also* expression, logical expression, mathematical expression.

Remote Access Services

A feature built into Windows NT and Windows 95 that enables users to log on to an NT-based LAN using a modem, X.25 connection, or WAN link. This feature is also known as Dial-Up Networking.

report group

1. The *standard* report groups in Historical Reporting are folders that contain the standard report templates. There are six standard report groups: Agent Performance, Configuration, Call-by-Call, Networking (M1 networking only), Others, and NCC (on the NCC only). 2. An administrator creates *custom* report groups in Access and Partition Management, adds them to partitions, and assigns the partitions to Historical Reporting users. Custom report groups do not contain standard report templates. Instead, they are folders that enable users who belong to the same group to share customized reports. Users can customize a standard template and save it in their group folder so that other members of their group can use the same customized report.

reporting supervisor

The supervisor who has primary responsibility for an agent. When an agent presses the Emergency key on the phoneset, the emergency call is presented to the agent's reporting supervisor. *See also* associated supervisor.

round robin routing table

A routing table that queues the first call to the first three sites in the routing table, then the second three sites, then the third three sites, and so on, until an agent is reserved at one of the sites. *See also* sequential routing table.

route
A group of trunks. Each trunk carries either incoming or outgoing calls to the switch. *See also* music route, RAN route.

router
A device that connects two LANs. Routers can also filter messages and forward them to different places based on various criteria.

routing table
A table that defines how calls are routed to the sites on the network. *See also* round robin routing table, sequential routing table.

RTD
Real-time displays

RTR
Real-Time Reporting

S

sample script
A script that is installed with the Symposium Call Center Server client. Sample scripts are stored as text files in a special folder on the client. The contents of these scripts can be imported or copied into user scripts to create scripts for typical call center scenarios.

SCM
See Service Control Manager.

script
A set of instructions that relates to a particular type of call, caller, or set of conditions, such as time of day or day of week. *See also* Master script, network script, primary script, secondary script.

script variable
See variable.

second-level threshold

The value used in display thresholds that represents the highest value of the normal range for a given statistic. The system tracks how often the value for the statistic falls outside this value.

secondary directory number

A DN defined on the agent's phoneset as a Centrex line for incoming and outgoing non-ACD calls.

secondary script

Any script (other than a Master, network, or primary script) that is referenced from a primary script or any other secondary script. There is no pegging of statistics for actions occurring during a secondary script. *See also* Master script, network script, primary script, script.

sequential routing table

A routing table method that always queues a call to the first three active sites in the routing table. *See also* round robin routing table.

server

A computer or device on a network that manages network resources. Examples of servers include file servers, print servers, network servers, and database servers. Symposium Call Center Server is used to configure the operations of the call center. *See also* client.

service

A process that adheres to a Windows NT structure and requirements. A service provides system functionality.

Service Control Manager

A Windows NT process that manages the different services on the PC.

service level

The percentage of incoming calls answered within a configured number of seconds.

service level threshold

A parameter that defines the number of seconds within which incoming calls should be answered.

Simple Mail Transfer Protocol

A TCP/IP protocol used to send messages from one computer to another on a network. This protocol is commonly used to determine the route for e-mail.

Simple Network Management Protocol

A systematic way of monitoring and managing a computer network. The SNMP model consists of four components:

- managed nodes, which are any device, such as hosts, routers, and printers, capable of communicating status to the outside world via an SNMP management process called an SNMP Agent
- management stations, which are computers running special network management software that interact with the Agents for status
- management information, which is conveyed through exact specifications and format of status specified by the MIB
- Management Protocol or SNMP, which sends messages called protocol data units (PDUs)

Simple Object Access Protocol

Technology for retrieving data through client PCs from the application server. SOAP provides a means of communication between applications running on different operating systems, with different technologies and programming languages.

site

1. A system using Symposium Call Center Server that can be accessed using SMI. 2. A system using Symposium Call Center Server and participating in Network Skill-Based Routing.

skillset

A group of capabilities or knowledge required to answer a specific type of call.

See also local skillset, network skillset.

skillset intrinsic

A script element that inserts information about a skillset in a script. Skillset intrinsics return values such as skillsets, integers, and agent IDs. These values are then used in queuing commands. *See also* call intrinsic, intrinsic, time intrinsic, and traffic intrinsic.

skillset priority

An attribute of a skillset assignment that determines the order in which calls from different skillsets are presented to an agent. When an agent becomes available, calls might be waiting for several of the skillsets to which the agent belongs. The server presents the call queued for the skillset for which the agent has the highest priority.

SMTP

See Simple Mail Transfer Protocol.

SNMP

See Simple Network Management Protocol.

SOAP

See Simple Object Access Protocol.

source site

The site from which an incoming network call originates. *See also* destination site.

standby

In skillset assignments, a property that grants an agent membership in a skillset, but makes the agent inactive for that skillset.

supervisor

A user who manages a group of agents. *See also* associated supervisor and reporting supervisor.

supplementary ACD-DN

A DN associated with a primary DN. Any calls to the supplementary DN are automatically routed to the primary DN. A supplementary DN can be a toll-free (1-800) number.

switch
The hardware that receives incoming calls and routes them to their destination.

switch resource
A device that is configured on the switch. For example, a CDN is configured on the switch, and then is used as a resource with Symposium Call Center Server. *See also* acquired resource.

Symposium Call Center Server call
A call to a CDN that is controlled by Symposium Call Center Server. The call is presented to the Incalls key on an agent's phoneset.

system-defined scripts
The Master_Script and the Network_Script (if NSBR is enabled). These scripts can be customized or deactivated by a user, but cannot be deleted. These scripts are This script is the first scripts executed for every local or network call arriving at the call center.

T

target site
See destination site.

TCP/IP
See Transmission Control Protocol/Internet Protocol.

telephony
The science of translating sound into electrical signals, transmitting them, and then converting them back to sound. The term is used frequently to refer to computer hardware and software that perform functions traditionally performed by telephone equipment.

Terminal services
An application that allows many computers to connect to a host computer, allowing input and output between the connected computer and its host.

threshold
A value for a statistic at which system handling of the statistic changes.

threshold class

A set of options that specifies how statistics are treated in reports and real-time displays. *See also* display threshold, pegging threshold.

time intrinsic

A script element that stores information about system time, including time of day, day of week, and week of year. *See also* call intrinsic, intrinsic, skillset intrinsic, traffic intrinsic.

Token Ring

A PC network protocol developed by IBM. A Token Ring network is a type of computer network in which all the computers are arranged schematically in a circle.

traffic intrinsic

An intrinsic that inserts information about system-level traffic in a script. *See also* call intrinsic, intrinsic, skillset intrinsic, time intrinsic.

transition mode

A skillset state in which the server presents already queued calls to a skillset. New calls queued to the skillset are given out-of-service treatment. *See also* night mode, out-of-service mode.

Transmission Control Protocol/Internet Protocol

The communication protocol used to connect devices on the Internet. TCP/IP is the standard protocol for transmitting data over networks.

treatment

See call treatment.

trunk

A communications link between a PBX and the public central office, or between PBXs. Various trunk types provide services such as Direct Inward Dialing (DID trunks), ISDN, and Central Office connectivity.

U

user-created script

A script that is created by an authorized user on the Symposium Web Client system. Primary and secondary scripts are user-created scripts.

user-defined script

A script that is modified by an authorized user on the Symposium Web Client system.

utility

A program that performs a specific task, usually related to managing system resources. Operating systems contain a number of utilities for managing disk drives, printers, and other devices.

V

validation

The process of checking a script to ensure that all the syntax and semantics are correct. A script must be validated before it can be activated.

variable

A placeholder for values calculated within a script, such as CLID. Variables are defined in the Script Variable Properties sheet and can be used in multiple scripts to determine treatment and routing of calls entering Symposium Call Center Server. *See also* call variable, global variable.

voice port

A connection from a telephony port on the switch to a port on the IVR system.

W

WAN

See also Wide area network.

Wide area network

A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local area networks (LANs). The largest WAN in existence is the Internet.

Index

A

Access and Partition Management
  access to 463
  adding Web Client users in 462
  and administrator privileges 463
  overview 16, 370
  partitions in 437
access classes 436
  access levels in 454
  and Contact Center Management 455
  and servers 455
  creating 453
access restrictions
  in Symposium Web Client 104
access rights 436
  assigning basic 438, 462
activating
  modified multicast rates 55
  modified RSM settings 56
  the Terminal Services License Server 192
activating or deactivating
  real-time statistics collection 49
Active Directory
  and domain controllers 75, 76
  and domain trees 77
  and forests of domain trees 78
  and Symposium Web Client uninstall 125
  backing up data 148
  computer name 79
  configuring the Terminal Services user account in 185
  database 81
  domain name 79
  forest in 79
  installing 75
  overview 75
  permissions 84
  problems with 525
  reinstalling 126
  server name in Symposium Web Client 105
  uninstalling 126
  verifying installation of 517
Active X control
  and Terminal Services 312
ad hoc agent to skillset assignments
  and Windows 98 411
  creating in assignment mode 414
ad hoc agent to supervisor assignments
  creating in assignment mode 405
addendum
  downloading latest 339
addresses
  Class D Internet Protocol 565
  multicast 565
  restriction for IP multicast 565
administrator
  privileges 463
  role of 371
administrator access
  defining typical 457
Agent Desktop Displays
  and multiple application servers 321
  and multiple language support 134
  and RDS 210, 321, 352
  and RSM 48
  and the IIS Lockdown procedure 210
  and the MSADC folder 332
  and the MSADC virtual directory 210
  and the refresh rate 195
  compatibility with versions of Symposium Web Client 321
  configuring 194
  configuring on the application server 164
  configuring the maximum number of agents 195
  configuring threshold colors for 195
  dependency on Real-Time Reporting 107
  installing 322
  installing and configuring on client PC 320

overview 18, 320, 371
problems upgrading 516
server component 107
tasks to perform before upgrading 355
upgrading 322
Agent Desktop Displays 4.5
compatibility with Symposium Web Client 4.0 323
agent details
editing 409
viewing 409
agent to skillset assignments 402
creating ad hoc 414
agent to supervisor assignments 402
creating ad hoc 405
agents
adding in Contact Center Management 423
All-Hosts Group 563, 564
and multicast data 562
All-Routers Group 564
and multicast data 562
application server
administrator password 552
and Symposium Web Client 19
and third-party software 27
communication ports on 42
communication problems with 512
computer name of 80, 552
configuring 164
configuring the event viewer log on 519
configuring to support multiple languages 141
hardware requirements for 26
installation tasks on 546
installing Sybase Open Client on 88
minimum refresh rate on 34
performance requirements for 32
receiving IP multicast address on 165
registering name of on DNS server 512
restarting after performing a platform migration 66
sending IP multicast address on 165
software requirements for 27
troubleshooting 517
uninstalling components from 122
application threshold classes
in Scripting 17
associated supervisors 467
Audit Trail
accessing 482
and monitored resources 484
overview 18, 371, 482

B

backing up
Active Directory data 148
Symposium Web Client data files 149
System State data 149
backups
scheduling 152
which data is backed up 147
backward compatibility
of client PCs 31
browser
configuring on client 292

C

changing
the IP address of Symposium Call Center Server 389
checklists
installation 536, 545
pre-installation 536, 537
Windows 2000 Server installation 550
Class D Internet Protocol addresses 565
Client Access Licenses
for Terminal Services 28, 68, 184, 543, 553
Client Access Licensing 68
client PC
communication ports on 42
coresidency on 31
hardware requirements for 29
installation tasks on 548
installing SOAP on 305
installing third-party controls on 309
installing third-party software on 288
modifying the HOSTS table on 513
modifying the LMHOSTS table on 513
software requirements for 30
third-party controls required on 317

troubleshooting display problems on 507
user privileges required on 313
client PCs
backward compatibility of 31
communication ports
on the application server and client PC 42
communication ports and partitions 36
computer name
Active Directory 79
Configuration
adding servers in 386
configuring resources in 391
downloading spreadsheets from 392
overview 16, 370, 384
spreadsheets 391
tasks in 384
using 399
configuration utility 54
configuring
application server to support multiple languages 141
Internet Explorer 5.5 on client PC 294
Internet Explorer 6.0 on client PC 297
Internet Explorer on client 292
Real-Time Reporting 167
the application server 164
Contact Center Management
adding agents in 423
adding supervisors in 424
adding users in 420
and access classes 455
and partitions 446
overview 15, 370, 402
cookies
and Internet Explorer 296
disabling 297, 298
overriding 297, 300
using advanced settings for 297
coresidency, on client PC 31
Crystal Reports Viewer
downloading 315
downloading files required by 316

D

data
preserving during uninstall 124
protecting 41
database
Active Directory 81
default printer
setting up 178
default values
clicking during RSM configuration 54
default web site
installing Symposium Web Client as 97, 106
directory path
changing for Agent Desktop Displays 327
display problems
troubleshooting 507
Distance Vector Multicast Routing Protocol 567
DMS switch
real-time statistics groups for 50
DNS
and Symposium Web Client 86
full name 79
DNS server
addresses 555
and Symposium Call Center Server 538
configuring 71, 527
registering application server name on 512
domain controller
and Active Directory 75, 76
setting the application server as 27
domain name
Active Directory 79, 105
domain trees
creating new 77
domains
Windows 2000 Server installation 556
downloading
data to Configuration spreadsheets 398
DVMRP 567

E

EBF11113 driver
updating 92, 345
e-mail notification in Historical Reporting 175
Emergency Help
configuring on the application server 164, 173
overview 18, 371
event viewer log
configuring on the application server 519
Everyone group
removing from the application server 201
exporting
files from Historical Reporting 181
scripts 193

F

File Allocation Table (FAT) partitions 41
forest
in Active Directory 79
forest of domain trees
creating new 78

H

hard disk space
confirming amount available 108, 329
requirements 108
hardware requirements
for the application server 26
for the client PC 29
high-level task flow 375
Historical Reporting
and partitions 446, 449
and partitions and supervisor/reporting agents feature 473
configuring 175
configuring on the application server 164, 175
e-mail notification in 175
exporting files from 181
overview 18, 371
historical reports
limit of simultaneous generated 34
host tables
configuring 528
configuring on the client PC 514
sample of LMHOSTS 515, 529
HOSTS table 528
adding the application server name to 513
manually updating 71
modifying on the client PC 513
sample 514, 529

I

ICERTDTrace
using to trace IP multicast data 518
icons
multicast and unicast in real-time displays 521
IGMP 567
IIS
installing 68
verifying installation of 517
IIS Lockdown 208
and the MSADC virtual directory 210
installing 211
installation
checklist 545
failure 111
skills required 24
TCP/IP 555
Terminal Services 554
time requirements 24
Windows 2000 components 553
installing
Active Directory 75
Agent Desktop Displays 322
IIS 68
language packs 133
new Symposium Web Client components 119
SMTP 68
Sybase Open Client 88
Terminal Services 68
Windows 2000 Server 64
installing Symposium Web Client
complete 107
custom setup 107
overview 62

Internet Assigned Numbers Authority 566
Internet Engineering Task Force 566
Internet Explorer 288
  and cookies 296
  configuring on client 292
  configuring version 5.5 on client PC 294
  configuring version 6.0 on client PC 297
  font size in 508
  security settings 294, 297
  selecting the language version in 114
  troubleshooting 507
  upgrading on the application server 113
Internet Group Management Protocol 567
Internet Information Services
  installing 68
interval-to-date 50
  in Agent Desktop Displays 195
IP address
  changing of Symposium Call Center Server 389
  for WINS 556
IP addressing
  dynamic 555
IP change utility 389
IP multicast addresses
  and mRcv.ini file 59
  for sending on Symposium Call Center Server 52
  receiving address on application server 165
  reserved 52
  restrictions 565
  sending address on application server 165
IP multicasting
  address 48
  implementing for Symposium Web Client 571
  overview 560
  requirements 571
  typing settings for in pre-installation checklist 539
IP port numbers
  default 52
IP Receive address
  configuring on the application server 168
IP Send address
  and networked Symposium Call Center Servers 168
  configuring on the application server 168

K

key code
  for Symposium Web Client 102
key codes 14
  and case sensitivity 102

L

LAN/WAN
  impact of unicast on 39
  multicast impact of application server on 37
language packs
  installing 133
  uninstalling 138
  viewing the version number of 138
  viewing those installed on server 138
language version
  selecting in Internet Explorer 114
languages
  changing the Regional Settings for 140
  support for multiple 128
languages supported in Symposium Configuration spreadsheets 396
license server
  activating for Terminal Services 192
licensing
  Terminal Services 313
LMHOSTS file name resolution
  activating 530
  activating on the client PC 515
LMHOSTS table 528
  manually updating 71
  modifying on the client PC 513
  sample 515, 529
local security policy
  verifying settings for 310
locales.dat file 141
localization 141
  and Symposium Web Client 128

M

M1 Data Extraction Tool
overview 16
using to connect to the switch 29
mail server
Smart Host name 176
manually copying files 150
maximum agents
for Agent Desktop Displays 195
MCast 58
section in the mRcv.ini file 59
MDAC 288
and clients with Windows 2000 289
installing on client PCs 289, 291
verifying version of 289
Mdac25.exe 291
Meridian 1
real-time statistics groups for 50
Meridian 1 Data Extraction Tool
spreadsheets for 394
Microsoft's Compatibility List 27
minimum requirements
Symposium Call Center Server 32
MOSPF protocol 568
moving window 50
in Agent Desktop Displays 195
mRcv application
starting 60
mRcv.exe utility 58
and the mRcv.ini file 59
mRcv.ini file 58
modifying 58
port numbers in 58
sample 59
MSADC folder
and Agent Desktop Displays 332
setting permissions on 355
MSADC virtual directory 210, 217
and IIS Lockdown 210
Msado15.dll 289
multicast
icons on real-time displays 521
multicast addresses 565
multicast data
sending and receiving 561
multicast group 561
multicast host group 561, 564
members of 565
permanent 564
transient 564
multicast hosts 563
multicast protocols 567
multicast rate 49, 53
activating modifications to 54, 55
activating new settings 54
and RSM 48
current transmission rate 55
default values 55
modifying 51
Multicast Receive utility 58
configuring 58
multicast routers 562
multicast routing methods 566
MulticastCtrl.exe 49, 50
multiple languages
changing the Regional Settings for 140
multipoint communications
and IP multicasting 560
traditional 560

N

name conflicts
while installing Active Directory 81
name resolution server
configuring 513, 527
NetBIOS domain
name of 81
network architecture
overview 22
network architecture overview 22
network components
of Symposium Web Client 18
networking
setting up in Windows 2000 554
NT File System (NTFS) partition 41
creating 64

O

OAM Timeout 170
OSPF protocol 568
Output Rate 53, 168

P

partitions
  and Access and Partition Management 437
  and Contact Center Management 446, 473
  and Historical Reporting 446, 449
  and Real-Time Reporting 446, 449
  and your call center 451
  assigning to users 439, 447
  compared to the supervisor/reporting agents feature 448
  creating 444
  creating NTFS 64
  FAT 41
  NTFS 41
  on the application server 550
  overview 451
  properties of 445
partitions and communication ports 36
partitions and supervisor/reporting agents feature
  and Historical Reporting 473
partitions and the supervisor/reporting agents feature
  and Real-Time Reporting 467
password
  and Scripting 191
  changing default when logging on to Symposium Web Client 379
  for Directory Services on application server 85
pcAnywhere 502
  and remote support 549
Performance Enhancement Packages (PEPs)
  downloading latest 549
performance requirements
  for the application server 32
permissions
  Active Directory 84
PIM protocol 568
platform migration
  restarting the application server after 66
port numbers 59
  for real-time statistics multicast 48
  in Symposium Web Client 42
  in the mRcv.ini file 58
Power User privileges 313
pre-installation
  worksheet 537
printer
  adding network when connected to other print server 180
  adding network with own IP address 178
  configuring for Scripting 192
  setting up default 178
Protocol Independent Multicast 568

R

real-time displays
  blank 521
  multicast and unicast icons on 521
Real-Time Reporting
  and IP multicast 561
  and MDAC 289
  and partitions 446, 449
  and partitions and the supervisor/reporting agents feature 467, 470
  and RSM 48
  configuration overview 165
  configuring 167
  configuring on the application server 164
  overview 17, 371
real-time statistics collection
  activating or deactivating 49
  interval-to-date 50
  moving window 50
real-time statistics groups
  for the DMS switch 50
  for the Meridian 1 switch 50
Real-time Statistics Multicast
  configuring on Symposium Call Center Server 545
  modifying settings 49

overview 48
testing the service 58
receiving
multicast data 563
recovery, from hardware failure 154
refresh rate
for Agent Desktop Displays 195
minimum on application server 34
Regional Settings
changing for multi-language support 140
Registry Values
clicking during RSM configuration 54
Remote Data Service
and Symposium Web Client 4.5 321, 352
reenabling on the application server 244
Remote Desktop Active X Control 314
remote support
from Nortel Networks 549
replication
and Symposium Web Client 65
Symposium Web Client data not replicated 65
Symposium Web Client data replicated 65
used to migrate Active Directory data 161
report groups
creating custom 441
custom 441
standard 441
requirements
for Symposium Call Center Server 32
Resource Reservation Protocol 568
resources
configuring in Configuration 391
restoring
data onto new server 155
Symposium Call Center Server data 159
Symposium Web Client data 153
Symposium Web Client data files 157
Symposium Web Client data onto the same server 158
reverting
back to a previous version of Symposium Web Client 159
routers
multicast 562
routing methods
multicast 566
spanning tree 566
RSM
activating new multicast rate settings 54
configuring on Symposium Call Center Server 545
multicast rates 48
overview 48
port numbers 48
restoring original values after a change 54
RSM configuration
and Symposium Call Center Server 49
default values 54
multicast rate 49
Registry Values 54
RSM settings
activating modifications to 54, 56
modifying 51
RSMConfg.exe 49, 51
RSVP protocol 568
RTD Multicast Configuration Utility 49
RTD Multicast Configuration window 51
RTD Multicast Controller Utility 49

S

scheduling
backups 152
Scripting
application threshold classes in 17
configuring on the application server 164, 183
configuring the default printer for 192
installing True DBGrid Pro 313
license requirements 313
overview 17, 370
password for 191
scripts
exporting 193
SDP service 55, 56
stopping and starting 54
troubleshooting 56, 57
security
in Symposium Web Client 104
selection criteria
and Historical Reporting 450
and partitions 450

sending
IP multicast data 561
serial number
for Symposium Web Client 102
servers
adding in Configuration 386
and access classes 455
Service Updates
downloading latest 549
setup
custom 107
order during installation 536
Terminal Services 554
Windows 2000 components 553
shared folders
creating on the application server 557
Simple Mail Transfer Protocol
installing 68
Simple Object Access Protocol. *See* SOAP
Smart Host name 176
SMTP 553
installing 68
SMTP server
configuring 176
verifying it is installed 175
SOAP 288, 305
installing on client PC 305
troubleshooting errors 531, 534
software requirements
for the application server 27
for the client PC 30
spanning tree routing method 566
spreadsheet
used for estimating CLAN/WAN impact 40
spreadsheets
downloading data to 398
downloading from Configuration 392
for the Meridian 1 Data Extraction Tool 394
in Configuration 384, 391
overview 395
problems uploading data from 520
using for configuring resources 394
using to upload data to Symposium Call Center Server 396
stand-alone web site
and default web site 576
Statistical Data Propagator
stopping and starting 54
supervisor access
defining typical 458
supervisor/reporting agents feature
about 464
and Contact Center Management 473
and Symposium Web Client components 469
assigning to Web Client users 466
compared to partitions 448
supervisor/reporting agents feature and partitions
and Historical Reporting 473
and Real-Time Reporting 470
supervisor/reporting agents matrix 584
supervisors
adding in Contact Center Management 424
and associated supervisors 467
supervisors and associated supervisors 467
switches
supported by Symposium Web Client 23
Sybase Open Client
installing 88
updating driver for 92, 345
upgrading 340
upgrading to v.12.5 88, 340
verifying version installed 88
Symposium Call Center Server
activating modified RSM settings on 56
and platform migrations 66
and Symposium Web Client 19
changing IP address of 389
communication problems with 517
installation tasks on 545
requirements 32
RSM configuration on 49
Symposium Call Center Server data
restoring 159
Symposium Call Center Server users 16, 23, 465
managing 402
Symposium Configuration spreadsheet
language support in 396
viewing the version number of 395
Symposium Configuration spreadsheets
problems downloading due to URLScan 391, 393

Symposium Web Client
about 15
access restrictions 104
and IP multicasting 571
and support for multiple languages 128
choosing web site types when installing 105
components of 15, 370
disk space requirements 108
installation overview 96
logging on for first time 378
name of application server 80
network components of 18
optional components when installing 107
port numbers in 42
repairing if damaged 116
reverting back to a previous version of 159
switches supported by 23
uninstalling 123
Symposium Web Client data
restoring 153
restoring onto new server 155
restoring onto the same server 158
Symposium Web Client data files
backing up 149
restoring 157
system requirements 26
System State data
backing up 149

T

TCP/IP
setup 555
TCP/UDP port numbers
about 41
Terminal Services
activating the license server 192
Active X Control required on client PCs 288
and Scripting 313
Client Access Licenses for 28, 68, 184, 543, 553
configuring the user account in Active Directory 185
Install Mode 100, 135, 526
installing 68
licensing 192, 313, 315
permissions 554
switching to Install Mode 90, 116, 119, 342
Terminal Services Client Access License 28, 68, 184, 543, 553
Terminal Services License Server
and communication with Terminal Services 27
Terminal Services Licensing 68
testing
the RSM service 58
third-party controls
installing on a client PC 309
problems downloading 516
required on the client PC 317
viewing the list of installed 319
third-party software
and Symposium Web Client installation failure 111
installing on client PCs 288
threshold colors
for Agent Desktop Displays 195
time to live 49
multicast value for your network 52
tombstone lifetime 153
Transform Rate 53, 168
troubleshooting
problems upgrading Agent Desktop Displays 516
True DB Grid Pro 288
True DBGrid Pro 312
installing for Scripting 313
TsInternetUser account
disabling 285
TTL 49

U

unicast
icons on real-time displays 521
impact of on the LAN/WAN 39
unicast sending
and IP multicast sending 561
uninstalling
Active Directory 126

language packs 138
Symposium Web Client components 122
the XML automated assignments feature 126
UNIX server
setting up as a print server 180
upgrading
Agent Desktop Displays 322
Sybase Open Client 88, 340
the XML automated assignments feature 351
uploading data
problems with 520
using Configuration spreadsheets 396
URLScan 208
and the Symposium Configuration spreadsheets 391, 393
installing 211
urlscan.ini file, editing 224
user name
modifying 463
users
adding Symposium Call Center Server 420
adding Web Client 462
different types of in Symposium Web Client 465
in Symposium Web Client 23
Symposium Call Center Server 16, 23, 465
Web Client 16, 23, 465
Windows 2000 23

V

version number
viewing in the Symposium Configuration spreadsheet 395
virtual directory
definition 576
installing Symposium Web Client as 106
setting Symposium Web Client up as 577
versus web site type 576
virtual networks
and IP multicasting 562
virus scan software
and Symposium Web Client 27

W

Web Client
password 410
user ID 410
Web Client user ID 424
Web Client users 16, 23, 465
adding in Access and Partition Management 462
web site types
definition 576
in Symposium Web Client 105
versus virtual directories 576
web sites
for downloading Service Updates and Product Enhancement Packages 549
webadmin 380, 463
and Configuration component 384
and Configuration spreadsheets 391
Windows 2000 Server
installation checklist 69, 550
installing 64
installing and configuring 67
installing on the application server 546
networking 554
requirements 67
Windows 2000 Server installation
and DNS server addresses 555
components 553
domains 556
IP addressing 555
Windows 2000 Service Pack 3
upgrading to 557
Windows 2000 users 23
Windows 98
and ad hoc agent to skillset assignments 411
Windows Backup Tool
using to back up data 151
Windows Installer 2.0, installing 101
WINS
IP address for 556
worksheet
pre-installation 537

X

XML automated assignments feature
installing 113
uninstalling 126
upgrading 351
XML files
sample files 427

Reader Response Form

Symposium Call Center Web Client
Product Release 4.5
Planning, Installation, and Administration Guide

Tell us about yourself:

Name: _____

Company: _____

Address: _____

_____

Occupation: _____ **Phone:** _____

1. What is your level of experience with this product?

   ☐ New user ☐ Intermediate ☐ Experienced ☐ Programmer

2. How do you use this book?

   ☐ Learning ☐ Procedural ☐ Reference ☐ Problem solving

3. Did this book meet your needs?

   ☐ Yes ☐ No

   If you answered No to this question, please answer the following questions.

4. What chapters, sections, or procedures did you find hard to understand?

   _____

   _____

   _____

5. What information (if any) was missing from this book?

   _____

   _____

   _____

6. How could we improve this book?

   _____

   _____

   _____

Please return your comments by fax to 353-91-756050, or mail your comments to Nortel Networks, Mervue Business Park, Galway, Ireland.

NORTEL NETWORKS™

Reader Response Form

Reader Response Form

Nortel Networks Symposium Call Center Web Client

Planning, Installation, and Administration Guide

Nortel Networks
Mervue Business Park
Galway, Ireland

Information is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

The process of transmitting data and call messaging between the Meridian 1, Symposium Call Center Server, and Symposium Call Center Web Client is proprietary to Nortel Networks. Any other use of the data and the transmission process is a violation of the user license unless specifically authorized in writing by Nortel Networks prior to such use. Violations of the license by alternative usage of any portion of this process or the related hardware constitutes grounds for an immediate termination of the license and Nortel Networks reserves the right to seek all allowable remedies for such breach.

Publication number:	297-2183-117
Product release:	4.5
Document release:	Standard 1.0
Date:	July 2003

NORTEL NETWORKS™