

# **BOSâNOVA Web System Administrator Guide**



## License and Document Information

Information in this manual is subject to change without advance notice. This manual is provided under the same license agreement which covers the corresponding software and hardware.

B.O.S. products are protected by copyright law and international trade agreements. No part of this product, including software, hardware, and manual may be reproduced or copied in any form or by any means without express written permission from B.O.S.

Unauthorized reproduction or distribution of this program or document, or any part thereof, is subject to criminal and civil penalties.

B.O.S. and BOSÂNOVA are trademarks of BOScom, Ltd.

It shall be inferred that all registered or trademarked products referenced in this manual retain their copyrights and trademarks.

© 2005 BOScom. All rights reserved. Printed in Israel.

Document Number **MM0122-13**; printed May 2006

## Contact Information

B.O.S., International Headquarters  
Rabin Building  
Teradyon Industrial Park  
Misgav 20179  
Israel

Tel: +972-4-990-7555

Fax: +972-4-999-0334

Email: [sales@boscom.com](mailto:sales@boscom.com)

[contactbos@boscom.com](mailto:contactbos@boscom.com)

For complete contact information and a list of Distribution Partners, see our web site:

<http://www.boscorporate.com/pages/distributors.asp?intGlobalId=2&iType=2>

Web site: <http://www.boscorporate.com>

# Table of Contents

## **BOSâNOVA WEB**

**SYSTEM ADMINISTRATOR'S GUIDE .....1**  
 Components of the BOSâNOVA Web System ... 3  
 Features of the BOSâNOVA Web System..... 3

## **SETTING UP THE BOSâNOVA WEB SERVER .....5**

**IBM iSeries-based Server..... 6**  
 Installing from the iSeries CD-ROM Drive ..... 6  
 Uninstalling BOSâNOVA Web from the Server .. 8  
 iSeries Utilities for BOSâNOVA Web Server ..... 9  
 Configuring Port Numbers ..... 10  
 Startup During Initial Program Load (IPL)..... 11  
 Configuring the BOSâNOVA Web Subsystem.. 12  
 Licensing with a Server License ..... 12  
 Licensing with a Processor Group License..... 13  
     Installing BNWPGLIC via Email .....14  
 Importing and Exporting a Server Setup..... 15

**PC-based Server ..... 15**  
 Prerequisites for Server Installation..... 16  
 Installing or Upgrading the BOSâNOVA Web Serv-

er ..... 16  
 Starting the BOSâNOVA Web Server ..... 18  
 Licensing BOSâNOVA Web..... 18  
 Exporting and Importing a Server Setup ..... 19

## **Uninstalling the Server..... 20**

## **CONFIGURING BOSâNOVA WEB ..... 21**

### **Configuration Flowchart ..... 22**

### **The Administrator Configurator ..... 23**

Logging in to the Administrator Configurator... 23

### **Server Configuration ..... 24**

HTTP Server Configuration..... 24  
 Proxy Server Configuration ..... 26  
 Server Security..... 28  
 SSL Configuration ..... 29  
     Overview of the SSL Configuration Process 29  
 Working with SSL Certificates..... 32  
     Generating a User Root Certificate ..... 33  
     Creating a New Certificate Folder ..... 33  
     Creating a Self-signed Certificate ..... 34  
     Creating a Certificate Signing Request (CSR)  
     35  
     Changing/Viewing Certificates ..... 38  
     Deleting Certificates ..... 38

<b>Host Connection</b> .....	<b>38</b>	<b>Group Configuration</b> .....	<b>54</b>
Configuring Host Connections .....	38	Creating Groups.....	54
Defining a New Host .....	38	Searching for a Group.....	55
Modifying an Existing Host .....	40	Copying an Existing Group .....	55
Deleting a Host .....	40	Modifying an Existing Group .....	56
<b>Session Configuration</b> .....	<b>40</b>	Deleting Groups .....	56
Display Session Profiles .....	41	<b>Integrity Check</b> .....	<b>57</b>
Creating a New Session Profile .....	41	<b>Server Monitor</b> .....	<b>57</b>
Copying a Profile .....	43	Active Server's Configuration Report.....	58
Modifying a Previously-configured Profile ..	43	Active Sessions Report.....	58
Deleting a Profile .....	43	Disconnecting Sessions.....	58
Menu Customization .....	44	Help Requests Report.....	59
Printer Session Profiles.....	44	Log Reports.....	59
Creating a New Profile .....	44	<b>Server Update</b> .....	<b>59</b>
Copying a Profile .....	47	Updating.....	59
Modifying a Previously-configured Profile Ses-	47	Licensing.....	60
sion .....	47		
Deleting a Profile .....	47		
Defining Dynamically-created Session Names.	48		
<b>User Configuration</b> .....	<b>49</b>	<b>CUSTOMIZING BOSâNOVA WEB</b> .....	<b>61</b>
Adding Users .....	50	<b>Overview</b> .....	<b>62</b>
Searching for a User .....	52	<b>Customizing the Appearance</b> .....	<b>62</b>
Copying an Existing User .....	52	Customizing the Background Image .....	62
Modifying an Existing User .....	52	Customizing Colors .....	62
Deleting Users .....	52	<b>Customizing Functionality</b> .....	<b>63</b>
Import Users from Host.....	53		
Clearing Users Private Configuration.....	53		
Downloading Trace Files .....	54		

<b>USERS DATA DEPLOYMENT .....</b>	<b>65</b>	<b>TROUBLESHOOTING .....</b>	<b>79</b>
<b>Logging in Data.....</b>	<b>67</b>	<b>Starting the Server in Interactive Mode .....</b>	<b>80</b>
Enabling Automatic Login with MS Windows....	67	Creating Java Programs Before Starting the Server	80
		Starting in Interactive Mode .....	81
<b>FIREWALL/PROXY SERVER CONSIDERATIONS ...</b>	<b>68</b>	<b>Playing Back Trace Screens .....</b>	<b>82</b>
<b>Firewall Provides Only Packet Filtering .....</b>	<b>69</b>	<b>Error Messages and Known Problems .....</b>	<b>83</b>
<b>Firewall Functions as a Proxy Server .....</b>	<b>69</b>	<b>Performance Issues .....</b>	<b>86</b>
BOSâNOVA Web Server Behind Firewall/Proxy		<b>FAQs .....</b>	<b>87</b>
Server .....	70		
Client Browser Behind Firewall/Proxy Server ...	70		
BOSâNOVA Web Server and Client Browser Be-			
hind Firewall/Proxy Server .....	71		
<b>SSL CONFIGURATION .....</b>	<b>73</b>	<b>INDEX AND NAVIGATION TIPS .....</b>	<b>88</b>
<b>The Need for SSL.....</b>	<b>74</b>	<b>Using the Index .....</b>	<b>89</b>
Public Key Encryption .....	74	Links to Index Headings.....	89
One-way Hash Functions.....	75	Navigation Tips .....	89
Digital Signatures.....	75		
Symmetric Cryptography .....	76	<b>Index.....</b>	<b>90</b>
Authentication .....	76		
<b>How SSL Works .....</b>	<b>78</b>		

# BOSâNOVA Web System Administrator's Guide

This guide contains instructions for installing and configuring the BOSâNOVA Web System and is designed for the **System Administrator**. For other information about BOSâNOVA Web, refer to the documents listed on the next page.

**Table 1: BOSÂNOVA Web Documentation Suite**

<b>Title</b>	<b>Format</b>	<b>Audience</b>	<b>Contents</b>
Installation Guide	Printed manual	Person installing BOSÂNOVA Web	A Quick Install sheet. The instructions contained on this sheet are often enough to successfully install BOSÂNOVA Web.
Online Help	HTML, opens in a browser	Administrator and users	Context specific help topics for every dialog box plus a general, fully indexed, HTML Help.
System Administrator's Guide	PDF, opens in Acrobat Reader	System Administrator	Instructions for installing, configuring, and uninstalling the BOSÂNOVA Web system.
User's Guide	PDF, opens in Acrobat Reader	End users	Instructions for running and configuring display and printer sessions, using JDTF, using macros, using MorphMaster, etc.
Release Notes	A .txt file available from the CD-ROM	System Administrator	Information about changes from previous versions, late-breaking news, and errata.

### Components of the BOSÂNOVA Web System

The BOSÂNOVA Web System includes two parts:

#### Server

Can be set up either on a PC (running Windows NT, 2000, XP, or 2003) or on an iSeries host that has a Java Virtual Machine available.

#### Client

End-users can run BOSÂNOVA Web display and printer sessions from a Web browser that supports the Java 2 platform, Enterprise Edition™. The user simply opens a Web browser and enters the IP address (or Domain Name) of the PC or iSeries acting as the BOSÂNOVA Web server. A Java applet automatically opens and a BOSÂNOVA Web frame is displayed in the browser window.

### Features of the BOSÂNOVA Web System

BOSÂNOVA Web is an enterprise-wide, centrally managed, Java-based solution that provides iSeries-to-desktop TN5250e GUI emulation and printing facilities. Computer users connected to an iSeries via an Intranet, Extranet, or the Internet access this application through any Web browser that supports the Java 2 platform, Enterprise Edition™.

The BOSÂNOVA Web server can be housed on an iSeries or a PC with Windows NT/2000/XP/2003, where it is maintained and managed. BOSÂNOVA Web's security features, based on SSL and industry-standard encryption mechanisms, ensure a safe and secure connection to the iSeries via the Web.

Part of BOSÂNOVA Web's power is the ability to control access via the use of different access points:

- Users running sessions over a normal (non-secure) connection use the http protocol and the non-secured http BOSÂNOVA Web server port.
- Users running sessions over a secure (SSL) connection use the https protocol and one of the https BOSÂNOVA Web server ports. This can be with or without client authentication.
- To access the User Configurator, use User.html
- For the Administrator Configurator, use Admin.html



The BOSÂNOVA Web System also:

- Provides iSeries display and printing emulation.
- Provides SQL-based data transfer.
- Employs the SSL protocol, industry-standard encryption algorithms, and BOSÂNOVA Web server login authentication to ensure secure and confidential communication between the server and clients.
- Includes MorphMaster, a tool which instantly converts legacy screens to full-color, mouse-sensitive screens complete with panels, popup windows, buttons, and more, all without altering the underlying legacy screens.
- Includes a full SCS Windows printing plug-in installed and initiated via the browser.
- Deploys automatically to all Internet or network-attached workstations using a Web browser.
- Includes a “thin” Web server that runs on the BOSÂNOVA Web server, eliminating the need for an existing Web server.

# **Setting Up The BOSâNOVA Web Server**

This section describes:

- IBM iSeries-based Server, p. 6
- PC-based Server, p. 15
- Configuring Port Numbers, p. 10

# IBM iSeries-based Server

Before you install the BOSâNOVA Web System, verify that the following requirements are met:

**Table 2: iSeries System Requirements**

<b>Operating System</b>	OS/400 V5R1 or higher
<b>Java Runtime Environment (JRE)</b>	JRE for Java 1.3 or higher
<b>Network Connection</b>	<ul style="list-style-type: none"> <li>• Ethernet or Token Ring adapter</li> <li>• TCP/IP</li> </ul>

---

**NOTE:** When using SCS printing and session names, OS/400 version V3R2, V3R7, or V4Rx with appropriate PTFs is required.

---

## Installing from the iSeries CD-ROM Drive

To install the BOSâNOVA Web Server on the IBM iSeries directly from the IBM iSeries CD-ROM drive:

1. Insert your BOS Connectivity CD-ROM into the IBM iSeries CD-ROM drive.
2. Log in as QSECOFR.

3. Type `LODRUN OPT01` in the command line. (This is the default name of the IBM iSeries CD-ROM drive.) The message “Restoring Objects from CD to library QTEMP. BOSâNOVA Web Version. Please wait...” appears on the message line. The Installation screen is displayed.
4. Enter the option number in the Your selection field:
  1. US BOSâNOVA web installation.
  2. Non U.S. BOSâNOVA web installation.
5. Press **Enter**. The License Acceptance screen is displayed.
6. Enter the option number in the Your selection field:
  1. I accept, continue installation.
  2. Cancel.
7. Enter one of these options in the Your selection field:
  1. Full installation  
The BOSâNOVA web server will be installed in the `/BNWbserver` directory.
  2. Evaluation installation  
The BOSâNOVA web server will be installed in the `/BNWvaluate` directory.

---

**NOTE:** If an evaluation version is already installed, you cannot install another evaluation version. However, you can license BOSâNOVA Web from the evaluation version.

---

8. Press **Enter**.

9. If you are upgrading, complete the steps “a” and “b”. If this is a new installation, continue with step 10.

- a. If an existing BOSÂNOVA Web installation is active, choose from one of the following options and press **Enter**.
  1. Continue the installation. The active BOSÂNOVA web will be closed.
  2. Cancel the installation.
- b. If an existing installation of BOSÂNOVA Web exists on the root directory, it will be renamed automatically. The new name is displayed on the screen. Choose to either continue or cancel the installation and press **Enter**.

10. Installation continues with one of these options:

- **New Installation**  
If the installation program does not find an existing BOSÂNOVA Web server on the IBM iSeries, default configuration is automatically installed.
- **Upgrade**  
If the installation program finds an existing BOSÂNOVA Web server or evaluation server, you can copy the configuration data from the existing installation to the new BOSÂNOVA Web directory.
  - If **either** an evaluation or a licensed BOSÂNOVA Web server exists.

- To copy the previous BOSÂNOVA Web server configuration data to the new BOSÂNOVA Web directory, enter **1**.
- To use the default configuration, enter **2**.
- If **both** a licensed and an evaluation BOSÂNOVA Web server exist.
  - To copy the previous BOSÂNOVA Web server configuration data to the new BOSÂNOVA Web directory, enter **1**.
  - To copy the previous configuration data from the evaluation server to the new BOSÂNOVA Web directory, enter **2**.
  - To use the default configuration, enter **3**.

11. If you are installing BOSÂNOVA Web for the first time on the iSeries, or if you choose not to copy a previous configuration, the BOSÂNOVA Web Ports Configuration screen is displayed.

	New Ports	Factory Default
<b>HTTP Server Ports:</b>		
Non-secured.....:	9999	8080
SSL.....:	9999	4443
SSL with User Certificate:	9999	4444
<b>Proxy Server Ports:</b>		
Non-secured.....:	9999	3334
SSL.....:	9999	7773

Figure 1: The Web Ports Configuration Screen

12. Either:
  - Press **Enter** to accept the default settings.
  - Reconfigure the ports and then press **Enter**.

13. Wait while the Java programs are created in the BOSÂNOVA Web installation directory. This can take up to 50 minutes.

## Uninstalling BOSÂNOVA Web from the Server

**WARNING:** Do not delete BOSÂNOVA Web objects until you are sure that you have removed all the BOSÂNOVA Web directories from the iSeries. You can select Remove BOSÂNOVA Web directory as many times as necessary to remove all of the directories. The Delete BOSÂNOVA Web Objects operation can be performed only once.

To uninstall BOSÂNOVA Web from the Server:

1. Enter **BNWuninst1** on the command line and press **Enter**.
2. Select either of the following:

### Remove BOSÂNOVA Web Directory

You must remove each directory, one by one, before you can delete the objects.

To locate the existing directories, type **CD/** on the command line and press **Enter**. Next, type **DSPLNK BNW\*** and press **Enter**.

- a. Enter **1** to remove existing BOSÂNOVA Web directories. If there are more than one

BOSÂNOVA Web directory, you must remove each individually.

- b. Press **Enter** to remove the specified directory. Removing a directory can take several minutes.
- c. If additional BOSÂNOVA Web directories exist, repeat this procedure.

### Delete BOSÂNOVA Web Objects

Regardless of the number of BOSÂNOVA Web directories that were installed on the IBM iSeries, there is only one set of BOSÂNOVA Web objects.


- a. Enter **2** to delete BOSÂNOVA Web objects.
- b. Press **F13** to display a list of objects to be deleted from the QGLP library.
- c. To save the objects on tape, type the following on the command line:  
**SAVOBJ OBJ(BNW\*) LIB(QGPL) DEV(TAP01)**

## iSeries Utilities for BOSÂNOVA Web Server

BOSÂNOVA Web Utility commands can be divided into two categories:

- those that can be entered on any command line
- those that are available only from the BOSÂNOVA Web Server Utilities menu

**Table 3: Utility Commands**

Command	Explanation
<b>BNW</b>	Displays the BOSÂNOVA Web iSeries Utilities menu
<b>BNWSTR</b>	Starts the BOSÂNOVA Web server.
<b>BNWSTR +  + *YES</b>	Opens the configuration page. The options are described below.
<b>BNWEND</b>	Stops the BOSÂNOVA Web server.

**Table 4: Commands Available only from the Server Utilities Menu**

Command	Explanation
<b>BNWCFG</b>	Configure the environment
<b>BNWCRT</b>	Create JAVA programs
<b>BNWLIC</b>	License BOSâNOVA Web
<b>BNWPGLIC</b>	Install Processor Group key
<b>BNWPORT</b>	Change the HTTP and proxy ports.
<b>BNWUNINST</b>	Uninstall BOSâNOVA Web
<b>BNWVER</b>	JAVA versions currently installed

## Configuration Page Options

In each case, follow the prompts.

### BOSâNOVA Web Installation Directory

Enter the complete path to the BOSâNOVA Web installation directory. For example:

[1] BOSâNOVA Web

## Java.version Property

Use this option if both Java 1.3 and Java 1.4 are installed and you want to run the server using Java 1.4.

Complete the entry with '1.4'

---

**NOTE:** To change the default Java version loaded automatically by the BNWSTR command, please contact BOS Technical Support.

---


## Additional class libraries


This field is reserved for updates and special features. Unless otherwise instructed, leave it blank.

## Configuring Port Numbers

To configure the HTTP Server port and the Proxy Server port numbers when the server is not active:

1. From an IBM iSeries workstation, open a display session and log on to the IBM iSeries where BOSâNOVA Web is installed.
2. In the command line, type **BNW** and press **Enter**. The server utilities menu is displayed.
3. Type **BNWPORT** and press **Enter**. The BOSâNOVA Web Server Ports Configuration screen appears.
4. There are two options:
  - Enter the port numbers and press **Enter**. (After entering new port numbers and **before** pressing

Enter, click  to reapply the existing, current port assignments.)

- Click  to reapply the default port configuration.

## Startup During Initial Program Load (IPL)

You can configure BOSâNOVA Web to start during the IBM iSeries's IPL.

**WARNING!** *This procedure is written for, and is to be executed by, a System Administrator or a senior programmer with extensive editing experience. This procedure changes the IPL sequence. Inexperienced personnel may cause severe problems.*

1. Check the QSTRUP system value to find the start-up program. Usually it is QSTRUP in the QSYS library.
2. Retrieve that program source with the command:  
**RTVCLSRC PGM(QSYS/QSTRUP) SRCFILE(QGPL/QCLSRC)**

The last lines of the source will appear as follows:

```
0048.00 QSYS/RTVSYVAL SYSVAL
        (QSTRPRTWTR) RTNVAR(&STRWTRS)
0049.00 IF COND(&STRWTRS = '0')
        THEN(GOTO CMDLBL(NOWTRS))
0050.00 CALL PGM(QSYS/QWCSWTRS)
0051.00 MONMSG MSGID(CPF0000)
0052.00 NOWTRS:
```

```
0053.00 RETURN
0054.00 CHGVAR VAR(&CPYR) VALUE(&CPYR)
0055.00 ENDPGM
```

3. Add a new line named BNWSTR after the line named NOWTRS. The result should appear as illustrated in line 52.01 below:

```
0048.00 QSYS/RTVSYVAL SYSVAL
        (QSTRPRTWTR) RTNVAR(&STRWTRS)
0049.00 IF COND(&STRWTRS = '0')
        THEN (GOTO CMDLBL(NOWTRS))
0050.00 CALL PGM(QSYS/QWCSWTRS)
0051.00 MONMSG MSGID(CPF0000)
0052.00 NOWTRS:
0052.01 BNWSTR
0053.00 RETURN
0054.00 CHGVAR VAR(&CPYR) VALUE(&CPYR)
0055.00 ENDPGM
```

4. Compile the program into QSYS lib with the command:  
**CRTCLPGM PGM(QSYS/QSTRUP) SRCFILE(QGPL/QCLSRC)**

During the next IPL, the BOSâNOVA Web server will run.




### Configuring the BOSÂNOVA Web Subsystem

By default, BOSÂNOVA Web runs from QBASE. To run it from a different subsystem on the IBM iSeries:

1. On the IBM iSeries command line, type **BNW** and press **Enter**. The server utilities menu is displayed.
2. type **BNWCFG** and press **Enter**. The following menu appears:

```
1  view the current BOSÂNOVA web configuration
2  Create a new environment (RECOMMENDED).
3  Use an existing JOBQ.
```

3. Select one of the options and press **Enter**. (For a detailed explanation of these three options, press .)

### Licensing with a Server License

This procedure describes licensing using a BOSÂNOVA Web Server License. See also “Licensing with a Processor Group License” on page 13.

**NOTE:** *Instead of using this procedure, BOS recommends licensing via the Server Update utility. See “Licensing” on page 60.*

To license BOSÂNOVA Web on an IBM iSeries server:

1. Ensure that the IBM iSeries supports JDK 1.3 or higher. OS/400 versions V5R1 and higher meet this requirement. For more information, contact IBM.
2. On the IBM iSeries command line, type **BNW** and press **Enter**. The server utilities menu is displayed.
3. On the command line, type **BNWLIC** and press **Enter**. This command runs the program **BNWLIC**. **BNWLIC** is installed on your iSeries during BOSÂNOVA Web server installation. A screen appears with the following options:
  1. Set Processor Group License
  2. Set Server License
4. Type **2** and press **Enter**. A screen appears with the following options:
  1. Display current license information.
  2. Get your customer ID.
  3. Enter the license key.
  4. Exit.
5. Type **1** and press **Enter**. The current license information (number of users, time remaining on the license, and local machine ID) is displayed.
6. Send the following information to BOS (at [sales@boscom.com](mailto:sales@boscom.com)):
  - The number of users you are authorized to license.
  - The Local Machine ID (from step 5).

- Serial number of the IBM iSeries where BOSâNOVA Web server is installed.
  - Your phone and fax numbers and email address.
7. The BOS sales department will generate three license keys and forward them to you.

---

**NOTE:** *There are three different client types reflecting the three different types of sessions: Spooler, Green screen, and GUI (green-screen with MorphMaster). Concurrent user sessions are counted according to the session type.*

---

When you receive the license keys:

- a. Repeat steps 1–2 above.
- b. Type **3** and press **Enter**.
- c. Enter the client type and press **Enter**.
- d. Enter the license key and press **Enter**.
- e. Repeat steps c–d for each client type license.

### Licensing with a Processor Group License

This procedure describes licensing using a Processor Group License. See also “Licensing with a Server License” on page 12.

1. Ensure that the program **BNWPGLIC** is installed on each IBM iSeries. This program can be installed either from the BOS CD-ROM or via the email

received from BOS Technical Support. (See the following section for instructions.)

2. On the IBM iSeries command line, type **BNW** and press **Enter**. The server utilities menu is displayed.
3. On the command line, type **BNWLIC** and press **Enter**.
4. Type **1** (Set Processor Group License) and press **Enter**.
5. Type **4** and press **Enter** to exit.
6. On the IBM iSeries command line, type **BNWPGLIC** and press **Enter**.
7. There are two options:
  - If you have your license key, type **1** (Add/Update Processor Group License) and press **Enter**. Then, enter the license key and press **Enter**.
  - If you do not have your license key, type **2** (Display Processor Group and Serial Number) and press **Enter**. Complete the form and submit it to one of the listed addresses. BOS will send you the license key. Then, repeat steps 5–6 and enter the license key.
8. Optionally, to display the license key information, type **DSPLICKEY PRDID(2510BNW)** and press **Enter**.
9. From the Administrator Configurator main menu, select **Host Connection**. The Host Connection screen opens. (See also “Host Connection” on page 38.)

10. Select the host from the table and click **Change**. The Host Properties screen opens.
11. Click **Update status**. BOSâNOVA Web updates the license status. The new status is displayed in the message displayed in the “Processor group license status” field.
12. Click **OK** to apply and save the new status.

---

**WARNING!** *If you exit from the Host Connection page without clicking OK, BOSâNOVA Web reverts to the old license status.*

---

### Installing BNWPGLIC via Email

---

To install BNWPGLIC via email:

1. Contact BOS Technical Support and request the BOSâNOVA Web Processor Group License by email. After you receive the email, continue with step 2.
2. On the IBM iSeries, enter the command **CRTSAVF QGPL/BNWPGSF**. This creates a Save file.
3. From the email, save the attached **BNWPGSF** file to your PC. Usually, that is possible by right-clicking the attachment and selecting Save as. Do not change the file name BNWPGSF.
4. From the computer, or any FTP client, copy in binary mode the **BNWPGSF** file into the **QGPL/BNWPGSF** Save file.

This can be done using a DOS FTP as follows:

- a. Open a Command prompt.
    - For Windows 95/98/NT, click Start > Run, and enter **command**.
    - For Windows 2000/XP, click Start > Run, and enter **cmd**.
  - b. Change the directory to the directory where the **BNWPGSF** file is located.
  - c. Type **ftp <AS/400 Ip address>** and press **Enter**.
  - d. Enter a valid User name and password.
  - e. Type **bin** and press **Enter**.
  - f. Type **put BNWPGSF QGPL/BNWPGSF** and press **Enter**.
5. On the IBM iSeries command line, enter the following. (This command restores the needed objects.)  
**RSTOBJ OBJ(\*ALL) SAVLIB(QGPL)  
DEV(\*SAVF) SAVF(QGPL/BNWPGSF)  
MBROPT(\*ALL) ALWOBJDIF(\*ALL)  
RSTLIB(QGPL)**
  6. Press **Enter**.
  7. On the IBM iSeries command line, type **BNW** and press **Enter**. The server utilities menu is displayed.
  8. On the command line, type **BNWPGLIC** and press **Enter**.

## Importing and Exporting a Server Setup

To import and export a BOSNOVA Web Server Setup when the Server is installed on an IBM iSeries:

1. In the command line of the IBM iSeries running BOSNOVA Web, enter a **SAV** command. For example, if saving BOSNOVA Web from the recommended /BOSNOVA Web directory to a standard iSeries tape TAP01, the command is:

```
SAV DEV('/QSYS.LIB/TAP01.DEVD') OBJ((' /
BSNserver')) DTACPR(*YES)
```

```
SAVOBJ OBJ(BNW*) LIB(QGPL) DEV(TAP01)
DTACPR(*YES)
```

2. On the IBM iSeries command line, use the corresponding commands: **RST & RSTOBJ**

---

**NOTE:** *Saved files can be used on other media instead of TAP01.*

---

## PC-based Server

Before installation, verify that the PC meets the following requirements:

<b>IBM iSeries Connection</b>	<ul style="list-style-type: none"> <li>• Ethernet or Token Ring adapter,</li> <li>• OS/400 V2R3 (or higher), and</li> <li>• TCP/IP line</li> </ul>
<b>PC</b>	Pentium 200 MHz or higher
<b>CD-ROM Drive</b>	Any type
<b>Internal Memory</b>	256 MB recommended (64 MB minimum)
<b>Hard Disk</b>	Minimum 17 MB available
<b>Network Connection</b>	Network-operable with TCP/IP protocol
<b>Operating System</b>	Windows NT, 2000, or 2003

### Prerequisites for Server Installation

---

Before installing the PC-based BOSâNOVA Web System:

1. Verify the server requirements.
2. Obtain the IP address or Domain Name of the PC.
3. Obtain the appropriate access permissions.
4. Check firewall and proxy server settings (see “Fire-wall/Proxy Server Considerations” on page 68).

---

**NOTE:** When using SCS printing and session names, OS/400 version V3R2, V3R7, or V4Rx with appropriate PTFs is required.

---

### Installing or Upgrading the BOSâNOVA Web Server

---

The server can be installed from the BOS Connectivity CD-ROM or you can download the installation program from the BOS web site and install from the download. However, the installation from the download is an evaluation version and is licensed for only 30 days.

---

**NOTE:** If a previous version exists, the download installation will upgrade it. If the previous version was licensed, the license will be applied to the upgrade.

---

Complete the following procedure for both a new installation and for an upgrade.

---

**WARNING about Upgrading!** When upgrading, if you do not want to overwrite your current installation, choose a different destination folder.

---

1. Verify that the PC meets the system requirements.
2. Close all applications.
3. Complete one of the following:
  - If you installing from the Connectivity CD-ROM, insert the CD-ROM. The CD-ROM boots automatically and the Install Options screen opens.
  - If you installing from a download file, double-click the .EXE file. The License Agreement is displayed. Continue with step 6.
4. Click either **Install your BOS Product** or **Evaluate your BOS Product**. The Setup Welcome screen is displayed.
5. Click **Next**.
6. Read the License Agreement. To install BOSâNOVA Web, you must click **Yes** to accept the License Agreement.
7. Enter your name and the company name and click **Next**. The Install Options screen is displayed.

---

**NOTE:** The company name is displayed in the Spooler properties menu.

---

8. Select either US Version or non-US Version. Installation omits this screen if installing from a downloaded file. A License Agreement screen is displayed.
9. Read the Sun Microsystems inc. Binary Code License Agreement and click **Yes** to accept the terms.

10. Either:

- Click **Next** to select the default directory, or
- Click **Browse** to select another destination directory and then click **Next**.

The HTTP Server Ports Configuration screen is displayed.

11. Either:

- Click **Next** to accept the default values, or
- Change the HTTP server port and/or SSL port values and then click **Next**.

The Proxy Server Ports Configuration screen is displayed.

12. Either:

- Click **Next** to accept the default values, or
- Change the Proxy server port and/or SSL port values and then click **Next**.

The Select Program Folder screen opens.

13. Either:

- Click **Next** to select the default BOSâNOVA Web program folder, or
- Select another program folder and then click **Next**.

The Check Install Information screen opens.

14. Review the settings and click **Next**. The installation process is launched. After approximately one minute, the Finish dialog box appears.

15. Select the checkbox to set the BOSâNOVA Web server to be an NT service.

---

**NOTE:** Alternately, the BOSâNOVA Web server can be set to be an NT service after installation by clicking Start > Run and entering the following command:

```
"<bosanova web server directory>\mk serv.exe" startall.exe  
For example: "C:\Program Files\BOS\jadvantage4\mk serv.exe"  
startall.exe
```

---

16. Click **Finish** to end the installation process.

### Starting the BOSÂNOVA Web Server

If it was set to be an NT service, when the PC boots-up, the BOSÂNOVA Web server starts automatically. A log file by the name **startall.log** is created in the BOSÂNOVA Web server directory every time this service starts. The log file details the Java command that was launched by the service.

If the server was not started automatically, you can start it from the start menu:

1. Select **Start > Programs > BOSÂNOVA Web**.
2. Select **Start All**.

A screen displaying an MS-DOS command prompt confirms that each server is running.

---

**NOTE:** *You must restart the BOSÂNOVA Web server after every license change or change of port configuration.*

---

To stop the service:

1. From the Administrator Configurator, select **Server Monitor**.
2. Click **Stop Server**.

---

**NOTE:** *This service cannot be stopped via the Windows Services Manager.*

---

### Licensing BOSÂNOVA Web

To license BOSÂNOVA Web for a PC-based server:

---

**NOTE:** *Instead of using this procedure, BOS recommends licensing via the Server Update utility. See “Licensing” on page 60.*

---

1. Install the full BOSÂNOVA Web version. For instructions on installation, see p. 16.
2. Run the License Wizard. (**Start > Programs > BOSÂNOVA Web > License Wizard**)
3. Select either:

#### **BOSÂNOVA Web Server License**

Click **Next** and continue with steps 4–7.

#### **Processor Group License**

Click **Finish** and continue with “Licensing with a Processor Group License” on page 13.

4. Click **Clipboard**. The information is copied to the clipboard.
5. Send the following information to BOS (at [sales@boscom.com](mailto:sales@boscom.com)):
  - The information pasted to the email from the clipboard.
  - The number of users you are authorized to license.
  - Your phone number, fax number, and email address.

6. The BOS sales department will generate three license keys and forward them to you. When you receive the license keys, rerun the License Wizard and type the license key in the appropriate Client-type Key field.

---

**NOTE:** *There are three different client types reflecting the three different types of sessions: Spooler, Green screen, and GUI (green-screen with MorphMaster). Concurrent user sessions are counted according to the session type.*

---

7. Click **Check**.

## Exporting and Importing a Server Setup

To export and import a BOSâNOVA Web Server Setup when the Server is installed on a PC:

1. Copy the following folders from the old Server's BOSâNOVA Web subdirectory and paste them into the new Server's BOSâNOVA Web subdirectory:

**Table 5: Subdirectory Folders**

Display	Groups	Profiles
Morphcfg	Images	JDTF
Traces	Kbmap	Macros
Users		

2. Copy the following files from the old Server's BOSâNOVA Web root directory and paste them into the new Server's BOSâNOVA Web root directory.

**Table 6: Root Directory Files**

Default.kbm	jmmexc.dat	Kbmap.kbm
morphconfig.cfg		secinf.dat
servers.jtn	systems.jtn	



## Uninstalling the Server

To uninstall BOSÂNOVA Web, you must stop the BOSÂNOVA Web server operation and run the Uninstall program.

---

***WARNING!*** Do not attempt to delete files or folders manually!

---

To completely remove the BOSÂNOVA Web System from either a PC-based server or from an IBM iSeries based server installed via a PC:

1. Select the BOSÂNOVA Web Uninstall program (**Start > Programs > BOSÂNOVA Web > BOSÂNOVA Web Uninstall**).
2. At the prompt, confirm the deletion/uninstall process.

# Configuring BOSâNOVA Web

This section includes:

- BOSâNOVA Web Configuration Flowchart, p. 22
- The BOSâNOVA Web Configurator, p. 23
- Server Configuration, p. 24
- Host Connection, p. 38
- Sessions Configuration, p. 40
- User Configuration, p. 49
- Group Configuration, p. 54
- Integrity Check, p. 57
- Server Monitor, p. 57
- Server Update, p. 59

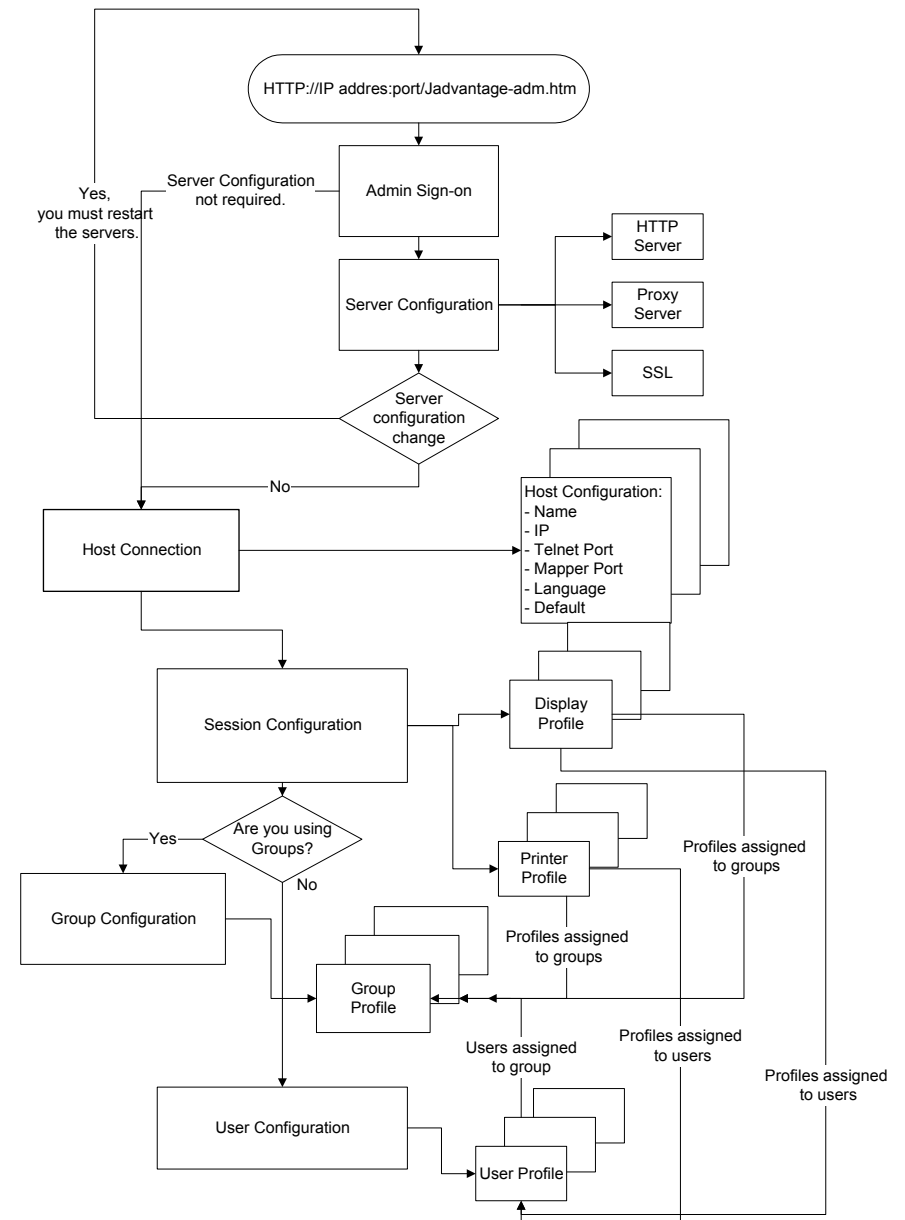
# Configuration Flowchart

## **WARNING about FIREWALLS!**

The BOSâNOVA Web Server may be located in front of or behind a firewall and/or proxy server. Depending on your system configuration and the type of firewall or proxy server you have, you may need to reconfigure.

For detailed information on configuration when a firewall or proxy server is present, "Firewall/Proxy Server Considerations" on page 68.

The following flowchart shows the required steps for configuring BOSâNOVA Web. All steps are described in detail in this section



# The Administrator Configurator

BOSâNOVA Web includes an Administrator Configurator and a User Configurator.

- Use the Administrator Configurator to add supported hosts, add and maintain users and groups, change user profiles, define session properties, etc.
- Use the User Configurator to perform certain limited functions such as setting the password and defining default sessions in addition to launching sessions.

Administrators are able, through the Administrator Configurator, to configure the following:

### **Server Configuration** (p. 24):

Opens the Server Configuration screen. Use this item to configure the HTTP and Proxy servers, and generate certificates for SSL secure connections.

### **Host Connection** (p. 38)

Opens the Host Connection screen. Use this item to add host systems to the access list and change their connection properties.

### **Group Configuration** (p. 54)

Opens the Group Configuration screen. Use this item to create and manage groups.

### **User Configuration** (p. 49)

Opens the User Configuration screen. Use this item to add, delete, or modify users.

### **Session Configuration** (p. 40)

Opens the Session Configuration screen. Use this item to add, delete, or modify profiles (for display and printer sessions).

### **Integrity Check** (p. 57)

Runs a test to see if any inactive profiles exist, that is, profiles assigned to host systems that have been deleted from the list in the host configuration screen.

---

**NOTE:** *The BOSâNOVA Web Administrator Configurator can be accessed only via the BOSâNOVA Web HTTP server.*

---

## Logging in to the Administrator Configurator

To log onto the Administrator Configurator:

1. From any PC, start a Web browser.
2. In the browser's Address field, enter:
  - a. The IP address or Domain Name for the IBM iSeries or PC acting as the BOSâNOVA Web server.
  - b. The Web server port number, prefaced with a colon (:).

- c. The index filename to access the Administrator Configurator (Admin.html)

for example:

http://194.90.180.80:8080/Admin.html

IP address or DNS    port    filename

The BOSâNOVA Web password screen opens.

3. The first time you log on, enter the default username and password:

Username: ..... admin

Password: ..... admin

4. Click **OK**. The BOSâNOVA Web Administrator Configurator main menu opens.

## Server Configuration

Use the Server Configuration screen to:

- Configure the HTTP Server
- Configure Proxy Servers
- Define which users have access to the BOSâNOVA Web Administrator Configurator
- Generate certificates for SSL secure connections
- Specify graphic format file extensions for image files

---

**NOTE:** Configure port numbers using either the Server Configuration page of the Administrator Configurator main menu or via the IBM iSeries BOSâNOVA Web **Server Ports Configuration** screen (see “Configuring Port Numbers” on page 10).

---

## HTTP Server Configuration

To configure an HTTP server:

1. From the Administrator Configurator main menu, select **Server Configuration**. The Server Configuration screen opens.
2. Click the **HTTP Server** icon. The HTTP Server Configuration screen opens.
3. Set the following:

### Port

This is the port users will access to run BOSâNOVA Web. The default is 8080.

### SSL Port

This is the port that will be used for secure connections. The default is 4443. For example:  
`https://194.90.189.80:4443/indexssl.htm`

### SSL with User Certificate Port

This is the port that will be used for users with secure connections. The default is 4444. For example:  
`https://194.90.189.80:4444/indexssl.htm`

### Log File Size

This is the maximum size of the log file. There are no limitations for the Log file size definition. We recommend using the default value which is 100KB.

A log file which reaches its size limit is saved to an archive. To view:

- the old log files, from the BOSâNOVA Web Administrator Configurator Server Monitor page, click **View old logs**.
- To view the current log files, from the BOSâNOVA Web Administrator Configurator Server Monitor page, click either **Proxy log** or **HTTP log**.

### Minimum free disk space (MB) / Maximum % ASP used

Old log files are saved until the server reaches a predefined disk space limit. To change the definition:

- For a PC based server, “Minimum free disk space (MB)” is the limit. If the server’s free disk space is less than the defined limit, then the oldest log file will be removed before a new file is saved in the archive.
- For an iSeries based server, “Maximum % ASP used” is the limit. If the % ASP used of the server is more than the defined limit, then the oldest log file will be removed before a new file is saved in the archive.

---

**NOTE:** The “Maximum % ASP used” is applicable only if the host’s Remote Command Server user name and password were set in the BOSâNOVA Web Administrator Configurator. See iSeries Remote Program calls on p. 39.

---

4. Select one or more of the following Log file options:

#### Log to File

If this option is selected, the log is written to the file `Httplog.html` in the root of the BOSâNOVA Web folder.

#### Log to Screen

In a PC server, if this option is selected, the log is written to the DOS box running the server applet. In an IBM iSeries server, the iSeries Log file holds all messages about connection activity on the BOSâNOVA Web server.

#### Debug Mode

If this option is selected, more detailed information is written to the log.

5. Select an **Encoding** option. Encoding determines the language of the text entered into configuration fields. Current to version 6.300, encoding is reflected in the applet in the Session Description only.
6. Specify Picture types. The default graphic formats appear under **Picture types**.
  - a. Ensure that the pictures to be viewed are located in the images/viewer directory on the server.
  - b. Ensure that the graphic formats to be entered in the **Picture types** box are supported by the browser.
  - c. Enter the graphic format extension in the **New Type** box.
  - d. Click **Add**.
  - e. If necessary, remove a graphic format by selecting a format extension and clicking **Remove**.

---

**NOTES:** *Ensure that unnecessary graphic formats are not added as they may reduce performance.*

---

7. Click **OK**.

## Proxy Server Configuration

A proxy server is a server that can redirect sessions to and from the host while providing SSL security. Configure a proxy server by defining access ports for display and printer session connections.

1. Verify that you have reconfigured existing firewall or proxy servers as needed.
2. From the Administrator Configurator main menu, select **Server Configuration**. The Server Configuration screen opens.
3. Click the **Proxy Server** icon. The Proxy Server Configuration screen opens.
4. Set the following:

### Port

This is the port that will be used for non-secure connections. The default is 3334.

### SSL Port

This is the port that will be used for secure connections. The default is 7773.

### Log File Size

This is the maximum size of the log file. A log file which reaches its size limit is saved to an archive. There are no limitations for the Log file size definition. We recommend using the 100KB default value.

5. Select one or more of the following Log file options:

### Log to File

If this option is selected, the log is written to the file `Httplog.html` in the root of the BOSâNOVA Web folder.

### Log to Screen

In a PC server, if this option is selected, the log is written to the DOS box running the server applet. In an IBM iSeries server, the iSeries Log file holds all messages about connection activity on the BOSâNOVA Web server.

### Debug Mode

If this option is selected, more detailed information is written to the log.

## 6. Configure the Client connection settings:

- While data is passing over a connection, the BOSâNOVA Web server continually restarts the countdown to timeout. Keep alive imitates this process. To prevent firewall disconnection and to keep idle sessions connected, choose a time interval from the **Send keep alive signal every:** field.
- To disconnect idle sessions after a specified amount of time, set **Send keep alive signal every:** to **Never** and choose a time interval from the **Connection timeout:** field.

---

**NOTE:** *If the network goes down, the server will take the amount of time set in the **Connection timeout** field before closing the device connection on the IBM iSeries and before removing the inactive sessions from the BOSâNOVA Web monitor session report.*

---

- The BOSâNOVA Web Client can be configured to automatically attempt recovery of a broken Telnet session. From the **Auto-reconnect timeout** dropdown box, select a time period. The BOSâNOVA Web Client will attempt to reconnect until the time period expires. To disable **Auto-reconnect timeout**, select **None**.

When network failure breaks the connection between the client and the server—for example, Internet failure—an automatic reconnect process is activated by the client applet. As soon as the disconnect is analyzed, the client tries to re-establish a TCP connection with the server proxy port. When the TCP connection is established, the BOSâNOVA Web proxy server tries to re-establish the Telnet session with the host.

---

**NOTE:** *The same session name—that is, the session name that was used before the disconnect—is used. In the case of Display sessions, to keep the same session name, the BOSâNOVA Web server must generate the session name. See “Creating a New Session Profile” on page 41.*

---

## 7. Click **OK** to save the settings.



## Server Security

Use the Server Security page to define which users have access to the BOSâNOVA Web Administrator Configurator.

1. From the Administrator Configurator main menu, select **Server Configuration**. The Server Configuration screen opens.
2. Click the **Server Security** icon. The Access to Administrator Configurator screen opens.
3. Configure the following parameters:

### Restrict ... access to the following IP addresses

Select the checkbox if access will be granted based upon the IP address. When clear, the IP address is ignored.

Enter the IP address and click **Add**. Repeat the process for each IP address from which access will be granted.

If the checkbox is selected but no IP address entered, only local access is possible. However, that restriction is only possible when the server is on a PC. When the server is on an IBM iSeries, at least one IP address must be entered.

### Restrict ... access to the following users

The list in the right pane contains all registered BOSâNOVA Web users and is derived from the list which appears on the User Configuration screen.

The list in the left pane includes the names of all users who are granted access to the Administrator Configurator.

Select a user from the right pane and click Add to grant that user access to the Administrator Configurator.

### Allow the user named ADMIN to login from remote stations

When clear, access from remote stations is permitted to all users defined above, via the IP addresses defined above, *except for* the user named ADMIN. This is a security precaution related to the fact that hackers often use the name ADMIN to try and breach security.

Select the checkbox to permit remote access to the user named ADMIN.

---

**NOTE:** *These parameters are cumulative (AND conditions). That is, if one IP address and five users are entered, all five users have access through the single IP address. Alternately, if five IP addresses and one user are entered, the single user has access through the five IP addresses.*

---

4. Click **OK**.

### SSL Configuration

To use the SSL protocol with BOSÂNOVA Web, you must install the server SSL certificate and configure port numbers for SSL-enabled server entry points. The Administrator Configurator includes some certificate management tools for:

- Generating and installing self-signed SSL server certificates.
- Generating a Certificate Signing Request (CSR) for an SSL server certificate and submitting it to a Certificate Authority (CA).
- Installing an SSL server certificate that was received from a CA.
- Managing several SSL server certificates at the same time.
- Generating and installing user certificates.

BOSÂNOVA Web provides the “BOSTest” SSL server certificate and a self-signed root SSL certificate for user certificate generation. These certificates may be used for testing purposes only.

### Overview of the SSL Configuration Process

Before you start the SSL configuration process, you must make decision about the following two issues:

#### 1. Selecting Server Certificate Type

If you know that only employees of your organization will access the BOSÂNOVA Web server then it’s sufficient to generate and install a self-signed SSL server certificate.

If, however, your system will be accessed from the Internet through, for example, an e-commerce system like amazon.com, then you should use a certificate signed by a well-known CA, for example, Thawte or VeriSign.

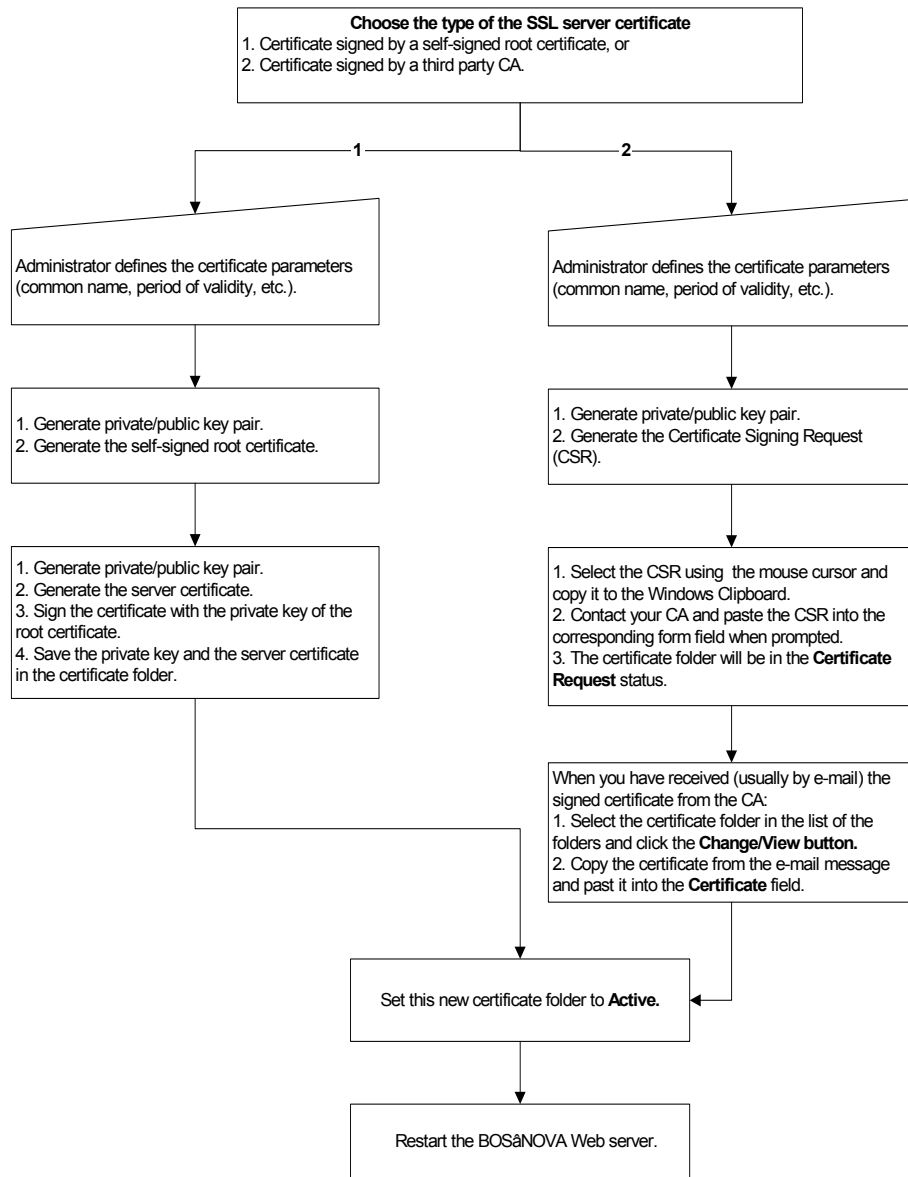
There are at least two reasons for using a well-known CA:

- Some users may not trust your server certificate and will not connect to the server.
- Even if users trust your server certificate, they will be warned by the browser that the received server certificate is signed by an unknown CA. In order to avoid this warning message, users must install the server root certificate in their browsers using the BOSÂNOVA Web User Configurator (BOSÂNOVA Web.htm).

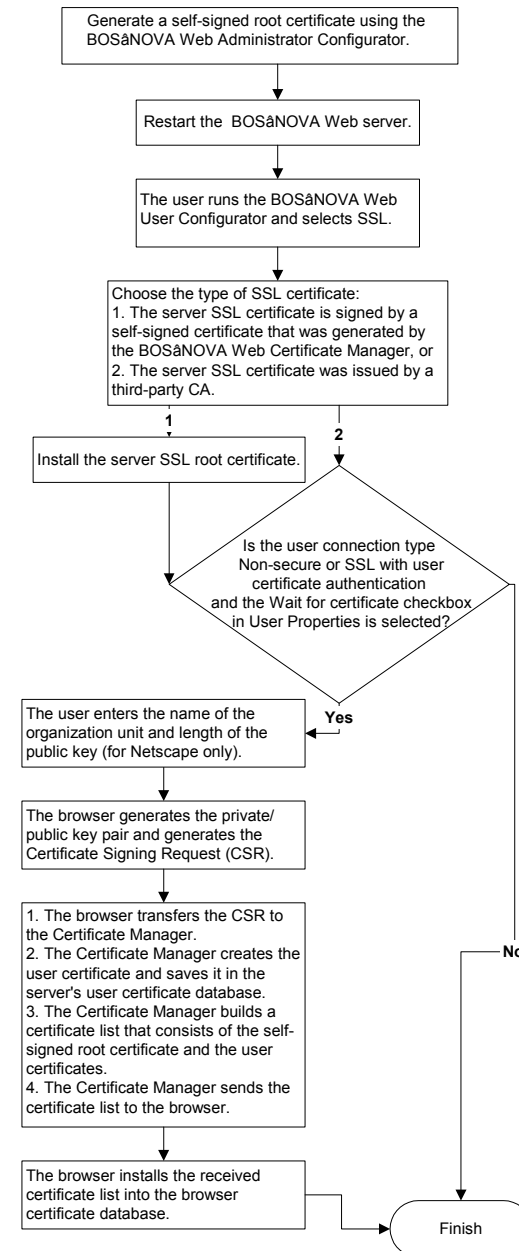
#### 2. Using User Certificate Authentication

User certificate authentication means that the BOS&NOVA Web server requests that a user's browser send certificate signed by the BOS&NOVA Web user root certificate when the user is connecting to the server. If the browser responds with a certificate, then the server checks it against the certificates kept in the server's database, and, if the certificate is valid, then the user will be allowed to connect. If the certificate is not valid or the browser cannot provide a suitable certificate, the server will immediately disconnect this station. This mechanism increases the security level of the whole system but requires some effort to certify each PC that the user is operating, so you have to decide if you really need it.

## Generating and Installing the Server SSL Certificate



## Generating and Installing the User SSL Certificate



### Working with SSL Certificates

BOSÂNOVA Web supports the SSL (Secure Sockets Layer) protocol. SSL provides a bi-directional, secure connection between the server and the client.

The SSL protocol generates the encryption keys and certificates necessary to provide secure connections with your BOSÂNOVA Web users.

The SSL protocol uses certificates to establish encrypted communication links. To support such communication links for BOSÂNOVA Web clients, you must create a server certificate, which contains identification information about the organization responsible for a Web site's content. The server certificate provides a way for users to authenticate your Web site and establish an SSL secure communication link.

There are two ways to create a server certificate:

- **Create a Self-signed Certificate:**  
This means that a company creates and signs its own certificate. This is fast and efficient and can be used if you only need to provide access to other members of the organization.
- **Obtain a Server Certificate from a Certificate Authority (CA):**  
A Certificate Authority (CA) is a mutually trusted, third-party organization (such as VeriSign or Thawte). The CA requires you to provide detailed identification infor-

mation about your company along with a Certificate Signing Request (CSR) before issuing a valid server certificate.

Once you receive a valid certificate file, you can install the server certificate.

With the BOSÂNOVA Web server, you can manage multiple server certificates. Each certificate, along with other necessary files, is stored in a certificate folder. All currently-defined certificate folders appear in the Administrator Configurator Certificate Folders screen (see p. 33).

Each folder must have a unique name. Each folder is listed with its status:

- **Usable:** The folder contains all necessary files and may be set as Active at any time.
- **Certificate Request:** The folder contains the private encryption key and Certificate Signing Request (CSR). It is not complete and cannot be set as Active.
- **Active:** The BOSÂNOVA Web server is using the certificate from this folder for SSL communication.

### Generating a User Root Certificate

---

With the current version of BOSâNOVA Web, you can use the user certificates that were signed by the special self-signed root certificate generated by the BOSâNOVA Web Certificate Manager.

To configure this root certificate:

1. Run the BOSâNOVA Web Administrator Configurator.
2. Log in as Administrator.
3. Select **Server Configuration > SSL Configuration**.
4. Select **Work with user SSL certificates**.
5. Click the **Root** button. The parameters of the currently-installed root certificate are displayed (can be used for tests only).
6. Click the **Create new** button. A new root certificate is created. The Certificate Manager uses subject parameters (server name, organization, locality) of the active server SSL certificate. The certificate is created for a 20-year validity period. All previously-created user certificates are removed.
7. Restart the BOSâNOVA Web server.

### Creating a New Certificate Folder

---

Use this screen to start the process of creating a new certificate folder for BOSâNOVA Web SSL secure connections.

1. From the Administrator Configurator main screen, select **Server Configuration**. The Server Configuration screen opens.
2. Select **SSL Configuration**. The Please Select screen opens.
3. Select one of the following options:
  - Work with server SSL certificates.
  - Work with user SSL certificates.
4. Click **OK**. The Certificate Folders screen opens.
5. Click **Add**. The New Folder screen opens.
6. Set the following:

#### Folder Name

Enter a name for the new certificate folder. The name may not include the following characters: \ / : \* ? < > |

#### Select an Action

Select which kind of certificate will be created:

- **Generate a Self-signed Root Certificate**  
If you only need to guarantee secure connections privately (for example, all users are members of the same organization that hosts the server site), you can generate a self-signed certificate. When

you select this option, you will be prompted to enter your identification information along with some certificate and encryption key parameters. After that, the program will generate the private/public encryption key pair and the CA (Certificate Authority) self-signed root certificate. (The key pair and certificate will be used in the next step.) The program will also generate the server SSL certificate signed by the CA private key.

- **Generate Certificate Signing Request (CSR)**

If you need to support users (clients) outside of your organization, you must be able to guarantee security through a valid third-party CA. When you select this option, you will be prompted to enter your identification information along with some certificate and encryption key parameters. After that, the program will generate the private/public encryption key pair and CSR in PKCS#10 format. The generated CSR will be displayed so you can select the text and copy it, via the Windows Clipboard, to the CA's certificate request form.

7. Click **OK**.

## Creating a Self-signed Certificate

---

If you selected the Self-signed root certificate option, the New Self-signed Certificate screen opens. Use this screen to enter the parameters needed for the private/public encryption keys and to generate the certificate.

---

**NOTE:** You may need to scroll down the screen to view all screen items and fields.

---

1. Set the following:

### Key Size

Select the size of the public/private encryption key from the list. The larger the key size, the more rigorous the encryption.

### Password

Enter a string. The string is used for encrypting the private keys in PKCS#8 format.

### Password Confirmation

Re-enter the password to guarantee accuracy.

### Root Certificate's Common Name

Enter a name for your CA (for example, your organization's name). This name will be shown in the list of the trusted CAs in the users' browsers once the CA certificate is installed there.

### Server Name

Enter the Internet name (Domain Name) of the computer on which the BOSâNOVA Web server runs (for example, www.mycompany.com). Note that you

won't be able to create an SSL connection using this certificate if you later rename your server computer. You can enter the BOSâNOVA Web server IP address if the users connect using an IP address instead of a domain name.

### Organization Name

Enter the full name of your organization.

### Organization Unit

Enter the name of the department in your organization that is responsible for running the server.

### Locality

Enter the name of the town or city where the BOSâNOVA Web server is located.

### State or Province

Enter the state or province where the BOSâNOVA Web server is located.

### Country

Select, from the list, the country where the BOSâNOVA Web server is located.

### Valid Not Before

Enter a starting date for the certificate. Use the lists to enter the month, day, and year.

### Valid Not After

Enter the last valid date for the certificate. Use the lists to enter the month, day, and year.

2. Click OK.

After your CA encryption keys and certificate are prepared, the program generates another pair of private/public encryption keys and the server X.509V1 certificate signed by your CA's private key. This certificate includes user parameters from your CA certificate.

If the process is successful, you will see the corresponding notification and you will be prompted to set this certificate folder as **Active**. (If you click **No**, the folder will be set as **Usable**.)

If you set this newly-created folder as **Active**, you must restart the BOSâNOVA Web server to force the server to use this certificate.

## Creating a Certificate Signing Request (CSR)

If you selected the CSR option, the New Certificate Signing Request screen opens. Use this screen to enter the parameters needed for the private/public encryption keys and to generate the certificate.

---

**NOTE:** You may need to scroll down the screen to view all screen items and fields.

---

1. Set the following:

### Key Size

Select the size of the public/private encryption key from the list. The larger the key size, the more rigorous the encryption.



### **Password**

Enter a string. The string is used for encrypting the private keys in PKCS#8 format.

### **Password Confirmation**

Re-enter the password to guarantee accuracy.

### **Server Name**

Enter the Internet name (Domain Name) of the computer on which the BOSÂNOVA Web server runs (for example, www.mycompany.com). Note that you won't be able to create an SSL connection using this certificate if you later rename your server computer. You can enter the BOSÂNOVA Web server IP address if the users connect using an IP address instead of a domain name.

### **Organization Name**

Enter the full name of your organization.

### **Organization Unit**

Enter the name of the department in your organization that is responsible for running the BOSÂNOVA Web server.

### **Locality**

Enter the name of the town or city where the BOSÂNOVA Web server is located.

### **State or Province**

Enter the state or province where the BOSÂNOVA Web server is located.

### **Country**

Select, from the list, the country where the BOSÂNOVA Web server is located.

### **Your e-mail Address**

Enter the e-mail address of the person who is responsible for the BOSÂNOVA Web server (for example, the BOSÂNOVA Web administrator). CA's normally send the signed certificate to this address.

### **Challenge Password**

This is a special password that will be required of you during your interactions with the CA.

### **Challenge Password Confirmation**

Re-enter the Challenge Password to guarantee accuracy.

2. Click **OK**. A summary of your Certificate Signing Request data is displayed.
3. Send the Certificate Signing Request to the CA authority:
  - a. Contact the CA (<http://www.thawta.com> or <http://www.verisign.com>). You will be asked to provide some documentation about your company. The CA will check that your company is registered in one or more countries and that its registered name is the same as that on the certificate. Once this is verified, the CA will send you the signed

certificate. Note that this process may take several days or even weeks.

- b. Upon receiving the certificate from the CA (usually via e-mail), install it on the BOSâNOVA Web server as follows:
  - i. Log on to the BOSâNOVA Web Administrator Configurator (Admin.html).
  - ii. Select **Server Configuration**.
  - iii. Select **SSL Configuration**.
  - iv. Select your certificate folder and click the **Change/View** button.
  - v. Paste the certificate that you received from the CA into the Certificate field. The text must include the lines "--BEGIN CERTIFICATE---" and "--END CERTIFICATE--".
  - vi. Click **OK**. If the process is successful, you will see the corresponding notification and you will be prompted to set this certificate folder as **Active**. (if you click **No**, the folder will be set as **Usable**). If you change the folder status to **Active**, restart the BOSâNOVA Web server (in order to force the server to use the new certificate).

The following is an example of a completed self-signed certificate:

### The 'BOSTest' Certificate

#### Common parameters

Parameter	Value
Version	0
Not valid before	Mon Nov 01 00:00:00 IST 1999
Not valid after	Sun Nov 01 00:00:00 IST 2020
Public key algorithm	RSA
Signature algorithm	md5WithRSAEncryption

#### Subject parameters

Parameter	Value
Common name	Jadvantage
Organization	Better On-line Solutions Inc.
Organization unit	Jadvantage Team
Locality	Scottsdale
State	AZ
Country	US

#### Issuer parameters

Parameter	Value
Common name	BOS Test CA
Organization	Better On-line Solutions Inc.
Organization unit	Jadvantage Team
Locality	Scottsdale
State	AZ
Country	US

### Changing/Viewing Certificates

---

The view or change a certificate:

1. From the Administrator Configurator, select **Server Configuration**. The Server Configuration screen opens.
2. Select **SSL Configuration**. The SSL Configuration screen opens.
3. Select an existing certificate folder from the list.
4. Click the **Change/View** button. The Certificate folder screen opens.
5. To set the folder as **Active**, click the **Yes** button.
6. Click **OK**.
7. If you turned the folder into Active, restart the BOSÂNOVA Web server.

### Deleting Certificates

---

To delete a certificate:

1. Select an existing certificate folder from the list.
2. Click the **Remove** button to delete it. A confirmation screen is displayed.
3. Click **OK** to confirm the deletion. The certificate folder is removed from the Certificate Folders screen.

## Host Connection

---

The Host Connection screen lists all connected host systems and connection parameters.

### Configuring Host Connections

---

Use the Host Properties screen to enter the connection parameters for a new IBM iSeries system or change the connection parameters for previously configured iSeries systems.

### Defining a New Host

---

To define a new host:

1. From the Administrator Configurator main menu, select **Host Connection**. The Host Connection screen opens.
2. Click **Add**. The Host Properties screen opens.
3. Set the following parameters:
  - System Name**  
Enter a descriptive or easy to remember name for the IBM iSeries.
  - IP Address**  
Enter the IP address for the IBM iSeries system.

### Telnet Port

Enter the IBM iSeries Telnet port number (the default is 23). This is the port on the IBM iSeries reserved for Telnet activity.

### Server Mapper Port

Enter the IBM iSeries mapper port number (the default is 449). This is the port on the IBM iSeries reserved as the server mapper.

### System Language

Select the appropriate language for the IBM iSeries from the dropdown list.

### iSeries Remote Program Calls

Enter the user name and password recognized by the host's Remote Command Server. BOSâNOVA Web uses the Remote Command Server:

- to activate various iSeries native programs and APIs
- to retrieve the status of a device which could not be used
- to check the Processor Group License status
- to retrieve the system status for %ASP

---

**NOTE:** *If you have licensed your system with a Processor Group License, clicking **Update status** will refresh the status message that appears in the "Processor group license status" field. This is the current status of the license at the host. (See "Licensing with a Processor Group License" on page 13.) You must click **OK** to save and apply a new status.*

---

### Case sensitive password

This setting must match the Host properties. When cleared, BOSâNOVA Web sends only uppercase letters to the Host. When selected, BOSâNOVA Web sends both uppercase and lowercase letters according to the user input. For example, "MyPassword" is different from "mypassword".

### Keep alive signal

Keep alive maintains a connection between an idle emulation session and the IBM iSeries. This parameter determines the type of Keep Alive signal sent from the BOSâNOVA Web client to the Host. Select either:

- **No-op**  
One of two minor buffers which track communication between the client and the IBM iSeries. This buffer can identify both idle and disconnected sessions.
- **Time-mark**  
BOS recommends this setting, the second of two minor buffers which track communication between

the client and the IBM iSeries. This buffer can identify both idle sessions and disconnected sessions.

4. Click **OK**. The Host Connection screen re-opens. The new host system appears in the list.

### Modifying an Existing Host

---

To modify an existing host:

1. From the Administrator Configurator main menu, select **Host Connection**. The Host Connection screen opens.
2. Select a host from the table and click the **Change** button. The Host Properties screen opens.
3. Modify the parameters as needed and click **OK**. The Host Connection screen re-opens.

### Deleting a Host

---

To delete a host:

1. From the Administrator Configurator main menu, select **Host Connection**. The Host Connection screen opens.
2. Select the host to delete and click the **Remove** button. The host is removed from the list.

---

**NOTE:** If you delete a host configuration, run an integrity check (p. 57).

---

## Session Configuration

---

A session profile is a way to define a type of session. This means that one session type, which may be appropriate for many users, need only be defined once. Session profiles support the definition of a dynamic session name; that is, a session name that can be created based on a user and/or group name.

With dynamic naming, the same session profile can be used to run many sessions by many users.

---

**NOTE:** There are three different licenses reflecting the three different types of sessions: Spooler, Green screen, and GUI (green-screen with MorphMaster).

---

Permission to add a new session profile depends upon the server license. If the server is licensed to support Green screen or GUI sessions, then you can add a display session. If the server is licensed to support Spooler sessions, then you can add a printer session.

## Display Session Profiles

Use the Display Session Profile screen to select or enter the parameters for a new display session profile, change the parameters of a previously configured profile, create a new profile or copy a profile (that is, create a new display session profile based on an existing one).

### Creating a New Session Profile

To create a new session profile:

1. From the Administrator Configurator main menu, select **Session Configuration**. The Session Configuration screen opens.
2. Click **Add**. The Session Profile Type screen opens.
3. Select **Display Session Profile**. The Display Session Profile screen opens.
4. Set the following:

#### Profile Name

This name will also appear in the Description column of the User's Sessions tables.

#### Session Name

Decide whether you want a specific name or a dynamically-created name for the session (this name will appear in the list in the Run Emulation screen):

- If you are using a specific name, select **Session Name** and enter the exact name. Note that

session names can contain numbers, letters, and the characters @ # \$ . \_ (but cannot begin with a number).

---

**NOTE:** If this field is blank, and the Advanced option is not selected, the host automatically defines the session name.

---

- If you are using a dynamically-created name, select **Advanced** instead. You must then click the **Advanced** button to open the Advanced Profile Properties screen to define exactly how the dynamic names will be created (for details, see p. 48).

#### System Name

Select, from the list, the IBM iSeries system that BOSâNOVA Web connects to when a user runs this session.

#### Display Parameters

Set Screen dimension and Color Support as needed.

#### Profile properties

Select the following options as needed:

- **Blinking cursor**  
If selected, the cursor will appear as a blinking rectangle.
- **Automatic log-off**  
If selected, a "log-off" macro is played when a display session window is closed. (Implemented only for Java 2 applet, client 5.x.)

- **Ruler**  
If selected, the user will have the option of displaying a ruler on the display session.
- **MorphMaster**  
If selected, this adds the option of viewing this profile in MorphMaster mode. See the overview on p. 45.

---

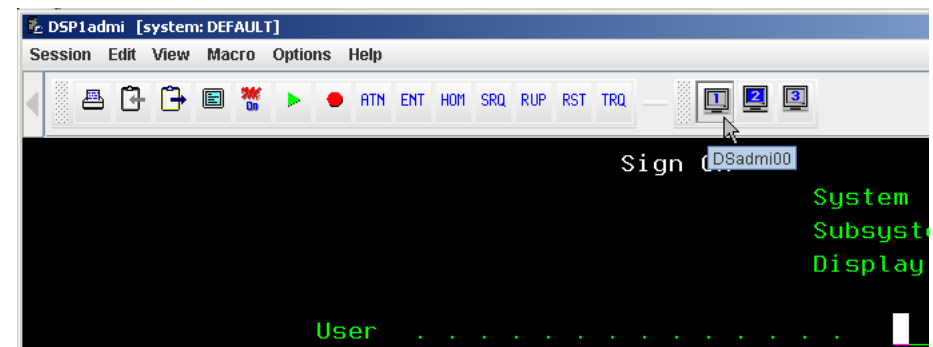
**NOTE:** The following option is available only when the **MorphMaster** checkbox is cleared.

---

- **Enable hot spots**  
If selected, when the pointer is over a function it changes to a hand and the background color of the function changes. When a user clicks within a hot spot, BOSâNOVA Web both transfers the function to the command line and performs the function.
- **Boxed error messages**  
If selected, all error messages also appear in a standard display box.
- **Right-click displays picture**  
If selected, right-clicking displays the associated picture and not the popup menu. To display the popup menu, depress the Shift key and then right-click.
- **Sign-on bypass**  
If selected, the user can skip signing-on to the

host. For example, Sign-on bypass enables you to use JDTF without having to log in to the IBM iSeries. However, the user must enter his Username and your Sign-on bypass password at the User Configuration screen.

- **Sessions toolbar**  
If selected, as illustrated below, an idle session can be accessed from the active session's window via the buttons on the toolbar.



- **Display alert before closing**  
If selected, a message is displayed before the a session is closed.
- **X for Input Inhibit indicator**  
The Input Inhibit indicator is the sign displayed in the lower left corner of of a Display Session while the iSeries is working. The default sign is II. When this option is selected, the sign is X.

- **Menu Customization**

Click this to open the Menu Customization screen.  
(See *Menu Customization*, p. 44.)

### Trace File

Select Record trace file to generate a trace file. Enter the filename.

5. Click **OK**. The session Profile Configuration screen re-opens. The new profile appears in the list.
6. Apply the profile to a group or to a user.

### Copying a Profile

---

To copy a profile:

1. From the Administrator Configurator main menu, select **Session Configuration**. The Profile Configuration screen opens.
2. Select a profile from the list and click the **Copy** button. The Display Session Profile screen opens with all the settings of the copied session profile.
3. Enter a name for the new profile and (if necessary) change any of the settings.
4. Click **OK**. The Profile Configuration screen re-opens. The new profile appears in the list.

### Modifying a Previously-configured Profile

---

To modify a profile:

1. From the Administrator Configurator main menu, select **Session Configuration**. The Session Configuration screen opens.
2. Select a profile from the list and click the **Change** button. The Profile Properties screen opens.
3. Change any of the settings as needed.
4. Click **OK**. The Profile Configuration screen re-opens. The new profile appears in the list.

### Deleting a Profile

---

To delete a profile:

1. From the Administrator Configurator main menu, select **Session Configuration**. The Profile Configuration screen opens.
2. Select a profile from the list and click the **Remove** button. The profile is removed from the list.

---

**NOTE:** *If you delete a display session profile, it automatically deletes from all users to which this profile is assigned. An active session is not interrupted, however.*

---



### Menu Customization

---

The BOSâNOVA Web System Administrator can customize the menus available to users.

1. From the Administrator Configurator main menu, select **Session Configuration**. The Profile Configuration screen opens.
2. Select **Display Session** and scroll down to the **Profile properties** field.
3. Click **Menus Customization**. The Menus Customization screen opens.
4. From **Menu Headings**, click the menu whose list you want to customize. The items available in that menu appear to the right of the Menu Headings list.
5. Click the menu items. Items with a **blue** background will appear on the menu. Items with a **white** background will not appear on the menu.

---

**NOTE:** Some items, such as Copy and Copy Mode, are dependent upon each other. Thus, if you deselect Copy Mode, Copy will automatically be deselected. Deselected menu items are removed from the menu, the toolbar, and the mouse right-click popup menu.

---

### Printer Session Profiles

---

Use the Printer Session Profiles screen to select or enter the parameters for a new printer session profile or to change the parameters of a previously-configured profile.

#### Creating a New Profile

---

To create a new profile:

1. From the Administrator Configurator, select **Session Configuration**. The Profile Configuration screen opens.
2. Click the **Add** button. The Profile Type screen opens.
3. Select **Printer Session Profile**. The Printer Session Profile screen opens.
4. Set the following identifying parameters:

##### Profile name

Enter a name. This name will appear only in the list on the Session Configuration screen.

##### Profile description

Enter a description. This entry will appear in the Description column of the User's Sessions tables.

##### Session name

Decide whether you want a specific name or a dynamically-created name for the session. This name will appear in the list on the Run Emulation screen:

- If you are using a specific name, select **Session Name** and enter the exact name. Note that session names can contain numbers, letters, and the characters @ # \$ . \_ (but cannot begin with a number).
- If you are using a dynamically-created name, select **Advanced**, instead. Click the **Advanced** button to open the Advanced Profile Properties screen to define exactly how the dynamic names will be created (for details, see p. 48).

### System Name

Select, from the list, the IBM iSeries system that BOSÂNOVA Web connects to when a user runs this session.

5. Select or clear **Associate to default Windows printer**. When selected, this session prints to the PCs default Windows printer.
6. Set the following printer parameters:

#### Message Queue

The host queue to which messages will be written.

#### Message Queue Library

Default \*LIBL.

#### Default Font ID

The font to be used if no font is specified by the application submitting the print job.

7. Set the following page parameters. These define the initial default page parameters, that is, the settings received when the user first opens a session. Thereafter, the user can redefine the page parameters unless **Overwrite user's parameters** is selected.

---

**NOTE:** To replace the user's page parameters with the parameters defined in this field, select **Overwrite user's parameters** and click **OK**. The System Administrator continues to control the page parameters as long as this option remains selected. To return control of the page parameters to the user, clear **Overwrite user's parameters** and click **OK**.

---

### Page Orientation

Select one of the following options:

- **Host**  
Means the host retains control over the page orientation, that is, the printer emulation applies the definition it receives from the host.
- **Landscape**  
Prints across the wide side of the paper.
- **Portrait**  
Prints across the narrow side of the paper.
- **COR (Computer Output Reduction)**  
Reduces the CPI and the LPI so that it fits on standard letter or A4 paper with landscape orientation.

- **Best Fit:**  
Means the PC printer retains control, but sets the orientation dynamically, based on the “best fit.”

### CPI (Characters Per Inch)

Select one of the following options:

- **Host:**  
Means the host retains control over CPI settings, that is, the printer emulation applies the CPI value it receives from the host.
- **Fixed numeric value**  
Selected from the dropdown list. Means the PC printer controls the CPI, which is set to a particular value for all print jobs.
- **Best Fit:**  
Means the PC printer retains control, but sets the CPI dynamically, based on the “best fit.”

### LPI (Lines Per Inch)

Select one of the following options:

- **Host:**  
Means the host retains control over LPI settings, that is, the printer emulation applies the LPI value it receives from the host.
- **Fixed numeric value**  
Selected from the dropdown list. Means the PC controls the LPI, which is set to a particular value for all print jobs.

- **Best Fit**  
Means the PC printer retains control, but sets the LPI dynamically, based on the “best fit.”

8. Using **Device Settings**, define the source of the print job’s definitions: the host or the emulation. If you select the emulation, you can select **Host Print Transform** and a printer type. This allows your host data to be sent directly to the printer without translation.
9. Assign a **Printer Driver** to the session. Select either:
  - **Current Windows driver**  
The session will print using the PC’s current printer driver.
  - **Special Driver > Custom**  
Use this option to distribute a customized printer driver to BOSâNOVA Web users.

---

**NOTE:** Custom printer drivers must carry the extension **.aps**. Create an **aps** folder and put the custom printer driver file into it.

---

To distribute a customized printer driver:

- i. Select **Special driver**.
- ii. Select **Custom**.
- iii. From the Driver’s language list, select a language.
- iv. Enter the printer driver file name. Be sure to include the **.aps** extension.

- v. Click **Apply new version**.
- **Special Driver > Factory**  
Select this option to assign a different factory standard printer driver to this session.

When the user opens a printer session, this printer driver is downloaded. Several confirmation messages escort the user through the download process.

---

**NOTE:** To refresh an existing custom printer driver, click **Update custom printer driver date to**. This gives the custom driver a new time stamp. When the BOSâNOVA Web System Administrator clicks **OK**, the printer driver download process starts over. The messages the user receives while downloading are also resent.

---

10. Click **OK**. The Session Configuration screen re-opens. The new profile appears in the list.
11. Apply the profile to a group or to a user.

### Copying a Profile

---

To copy a profile:

1. From the Administrator Configurator main menu, select **Session Configuration**. The Profile Configuration screen opens.
2. Select a profile from the list and click the **Copy** button. The Printer Session Profile screen opens with all the settings of the copied session profile.
3. Enter a name for the new profile and (if necessary) change any of the settings.

4. Click **OK**. The Profile Configuration screen re-opens. The new profile appears in the list.

### Modifying a Previously-configured Profile Session

---

To modify a profile:

1. From the Administrator Configurator, select **Session Configuration**. The Profile Configuration screen opens.
2. Select a profile from the list and click the **Change** button. The Profile Properties screen opens.
3. Change any of the settings as needed.
4. Click **OK**. The Profile Configuration screen re-opens. The new profile appears in the list.

### Deleting a Profile

---

To delete a profile:

1. From the Administrator Configurator, select **Profile Configuration**. The Profile Configuration screen opens.
2. Select a profile from the list and click the **Remove** button. The profile is removed from the list.

---

**NOTE:** If you delete a Printer Session profile, it is automatically deleted from all users to which this profile is assigned. An active session is not interrupted, however.

---

### Defining Dynamically-created Session Names

For both Display and Printer Session Profiles, you can decide whether you want a specific session name or a dynamically-created session name. This name will appear in the Log-in screen. When an explicit name is not defined, the **Advanced Profile Properties** screen is used to configure how dynamic display or printer session profile names are created.

1. From the Administrator Configurator, select **Session Configuration**. The Session Profile Configuration screen opens.
2. Click **Add**. The Profile Type screen opens.
3. Select the desired session profile. The Session Profile screen opens.
4. In the Session name box, select **Advanced**.
5. Click the **Advanced** button. The Advanced Profile Properties screen opens.
6. Select one of the following:

#### **Use the First 9 Characters of the User Name**

When selected, the first nine characters of the user name will become the prefix for the session name.

#### **Use the First 9 Characters of the Group Name**

When selected, the first nine characters of the group name will become the prefix for the session name.

### Generate the Session Name Automatically

If this option is selected, the session name will be generated based on the table further down on the screen. Define the number of characters and the type of session prefix. A maximum of ten characters are allowed, including all 3 lines.

7. Set the length of the session name. The maximum length is 10 characters.
8. For each line:
  - a. Select one of the options from the dropdown list.
    - **User Name**  
BOSâNOVA Web will take the specified number of characters from the beginning of the username.
    - **Group Name**  
BOSâNOVA Web will take the specified number of characters from the beginning of the group name.
    - **Text**  
BOSâNOVA Web will take the string you enter.
    - **None**  
Select **None** if you are not using this line. This option may be used in lines 2 or 3 only.
  - b. Enter the number of characters or the string for that option.

---

**NOTE:** BOSâNOVA Web sequentially adds numbers at the end of the session names if (a) the maximum length of the session name as defined in step 7 is longer than (b) the actual session name implied by the entries in the three fields. For example, if the length of the session name is defined as 10, and 3 characters are defined in each of the three fields, BOSâNOVA Web automatically adds a number in the available tenth character space. Generally, BOS recommends not allowing this to occur.

---

For example, if the first line was set to the first three letters of the group name, the second line was set to the first three letters of the username, and the third line set to text, you could have an automatically-generated session name such as ENGJOEDSP1, where ENG is from the group name *Engineering*, JOE is from the username *JoeWillard*, DSP is text to represent a display session, and 1 is the appended session number, automatically added by BOSâNOVA Web.

---

**NOTE:** The name will be built starting with the instruction in the first line, then the second, etc.

---

9. Click **OK**. The Profile Session screen re-opens.
10. Click **OK** again to save the changes.

## User Configuration

---

The BOSâNOVA Web administrator can set up users individually, defining the properties of each user, the profiles (sessions) the user can connect to, and the user's access permissions. This is ideal when each user has different needs and requirements.

You can also add the user to a Group to give access to a group's profiles, and, if necessary, assign additional profiles to a specific user.

In the User Properties screen, you can enter the configuration properties for a new user, change the properties of an existing user, or remove a user from the list.

With the User Configuration screen you can:

- Add a user with username and password
- Assign permissions
- Set up a secure connection for the user
- Assign profiles to users

### Adding Users

---

To add users:

1. From the Administrator Configurator main menu, select **User Configuration**. The User Configuration screen opens.
2. Click **Add**. The User Properties screen opens.
3. In the **User ID** box, enter these parameters:

#### **Username**

Enter the name used to log in to BOSâNOVA Web.

#### **Full Name**

Enter the user's full name to help you identify and manage the user. This name appears in parentheses next to the BOSâNOVA Web username in the User Configuration screen.

#### **Check password via host**

Select this checkbox to use the host's sign-on services for password verification.

---

**NOTE:** Selecting **Check password via host** establishes automatic sign-on bypass to the host.

---

#### **Password**

Enter the password the user uses to log in to BOSâNOVA Web.

#### **Verification**

Enter the user password again for confirmation.

4. Assign the **User Permissions** by selecting one of the following options:

#### **Administrator**

With or without Global morph configuration, all permissions are enabled.

#### **Guest**

None of the permissions are enabled.

#### **Custom**

Permissions can be customized by clicking Advanced.

---

**NOTE:** Selecting **Global morph configuration** enables the administrator to configure MorphMaster for all users. However, users who have been assigned the MorphMaster customization permission are able to override the administrator's global configuration and personalize their MorphMaster settings. In addition, if the administrator wants to define **only** his own MorphMaster settings, he must clear Global morph configuration.

---

5. In the **Connection Type** box, select the type of connection (Non-secure, SSL, or SSL with authentication, see <Italic>Server Security on page 28). Optionally, select from the following:

#### **Wait for Certificate**

Indicates that the connection type will not go into effect until the user certificate is installed on the user's browser.

### Restrict Access

When selected, the user is able to log-on only to IP addresses that are listed as authorized. First, enter the IP address in the field. Then, click Add.

6. To customize the user permissions, select **Custom** and click **Advanced**. The User Permissions screen opens.
  - a. In the User Permissions screen, the BOSâNOVA Web administrator can allow or deny specific permissions to the user. To permit the user to perform one of the listed actions (such as allow to configure password), or to give the user access to a specific module (such as keyboard mapping), select the option. When selected, the option is marked by an **X**, meaning that the user is permitted to perform the action.
  - b. In the User Permissions screen, select the **Allow JDTF** option to permit the user to use JDTF. To permit the user to perform one of the listed actions, select the specific JDTF checkbox. When selected, the option is marked by an **X**, meaning that the option is accessible and permitted for use by the user.
7. Enter the **Maximum number of sessions** this User is allowed to open.
8. Select or clear **Start all sessions after login**. When selected, at log-in, if the user selects the “Run default

sessions” checkbox, BOSâNOVA Web automatically opens all default sessions.

9. Using the options in the Group Configuration box, determine if the user will be defined as a member of an existing group.
  - To assign the user to a group, select a group from the **Available groups** list and click **Add**. The selected group appears under the Groups assigned to user list.
  - To remove the user from a group, select the group from the **Groups assigned to user** list and click **Remove**.

---

**NOTE:** *The List of profiles on each side shows the profiles of the selected group.*

---

10. Use the **Profile Configuration** box to assign additional profiles to specifically this user, over and above any profiles assigned via the group.
  - To assign a profile to the user, select a profile from the **Available profiles** list and click **Add**.
  - To remove an assigned profile, select the profile from the **Profiles assigned to user** list and click **Remove**.
11. Configure **Diagnostics**. You may need to record a telnet trace when a User is experiencing problems with a session. Select this checkbox and assign a maximum size to the .trc file that is created.



12. Click **OK**. The User Configuration screen re-opens.  
The new username appears in the list.

### Searching for a User

To search for a user:

1. From the Administrator Configurator main menu, select **User Configuration**. The User Configuration screen opens.
2. Enter the name of the user in the Find field and click **Find**. The user is selected in the user configuration list.

### Copying an Existing User

To create a new user based on an existing one:

1. From the Administrator Configurator, select **User Configuration**. The User Configuration screen opens.
2. Select a username from the list and click the **Copy** button. The User Properties screen opens with all the settings of the copied user.
3. Give a new name to the user and then change other settings, as needed.

4. When you are finished making changes, click **OK**.  
The User Configuration screen re-opens.

### Modifying an Existing User

To modify an existing user:

1. From the Administrator Configurator main menu, select **User Configuration**. The User Configuration screen opens.
2. Select a username from the list and click **Change**.  
The User Properties screen opens.
3. Change the settings as needed.
4. When you are finished making changes, click **OK**.  
The User Configuration screen re-opens.

### Deleting Users

To delete a user:

1. From the Administrator Configurator main menu, select **User Configuration**. The User Configuration screen opens.
2. Select a username from the list and click **Remove**.  
The username is removed from the list.

### Import Users from Host

You can import users, from the list of users located on the host, to the BOSÂNOVA Web User Configuration list.

1. From the Administrator Configurator main menu, select **User Configuration**. The User Configuration screen opens.

---

**NOTE:** Only a host user with administrative privileges can import users from the host.

---

2. In the Import users from host area, enter:

**Username**

The host username.

**Password**

The host password.

**Appropriate host**

Select the host with the target list.

3. Click **Import**. The Import Users from Host screen opens. The list shown displays all host users that are not in the BOSÂNOVA Web Users List.
4. From the Host Users list, select the users to be added to the BOSÂNOVA Web User Configuration list.
  - Click **Select All** to import all the user names in the host list.
  - Use **Find** to locate specific users.

---

**NOTE:** To multi-select, hold down **Ctrl** and click the user names. To select a number of contiguous user names, select the first name, hold down **Ctrl** and **Shift**, and select the last name.

---

5. Click **OK**.

A profile is created for each imported user and is added to the BOSÂNOVA Web Users list. The profile is assigned the default configuration along with Check password via host.

### Clearing Users Private Configuration

To purge the private settings defined over the configuration files by a user:

1. From the Administrator Configurator main menu, select **User Configuration**. The User Configuration screen opens.
2. Click **Files List**. An advisory informs you that the process may take some time.
3. Click **OK** to continue. The **Users Private Files** screen appears.

---

**NOTE:** Under **Sort by**, select a radio button to sort either by user name, file name, or file type.

---

4. There are two possibilities:

To delete **individual** files:

- i. Select the checkboxes of the files.
- ii. Click **Delete Selected Files**.

To delete **multiple** files according to type and user:

- i. From the first drop down menu, choose a type of file.
- ii. From the second drop down menu, choose the user whose files you want to delete.
- iii. Click **Delete Files Matching this Description**.

### Downloading Trace Files

To download and save a trace file:

1. From the Administrator Configurator main menu, select **User Configuration**.
2. Click **Files List**. An advisory informs you that the process may take some time.
3. Click **OK** to continue. The **Users Private Files** screen appears.
4. Files are listed in the middle, **File Name**, column. There are two options:
  - First, click the file. The file opens in a new browser window. Then, save the file.
  - Right-click the link and select **Save target as**.

## Group Configuration

With BOSâNOVA Web, you can organize users into groups. A group is a set of users who need the same access to hosts and the same session types and profiles. The BOSâNOVA Web administrator must first create session profiles, then create users, and then create a group definition.

### Creating Groups

To create a group:

1. From the Administrator Configurator main menu, select **Group Configuration**. The Group Configuration screen opens, where all currently defined groups appear in a list.
2. Click **Add**. The Group Properties screen opens.
3. Set the following:

#### Group Name

Enter a descriptive name that represents the function or purpose of the group (for example, Sales for all sales personnel in the organization).

#### Profile Configuration

All defined profiles appear on the right under the Available profiles list.

- To **assign** a profile for this group, select a profile from the **Available profiles** list and click the **Add** button. The profile now appears under the Profiles assigned to group list. This means that all users defined as members of this group automatically receive access to the session defined in that profile. Continue adding profiles as needed.
  - To **remove** profiles from the group definition, select a profile from the **Profiles assigned to group** list and click the **Remove** button. The profile now appears back under the Available profiles list.
4. When all profiles have been selected for the group, scroll down to User configuration. All defined users appear on the right under Available users.
- To **assign** a user to this group, select a username from the **Available users** list and click **Add**. The username appears under the **Users assigned to group** list.
  - To **remove** users from the group definition, select a username from the **Users assigned to group** list and click **Remove**. The profile appears back under Available users list.
5. Select or clear **User login required**. If GroupID is customized in the applet page, and this is cleared, then the user login screen is omitted. The applet automatically loads the sessions screen.

6. Click **OK**. To the Group Configuration screen is displayed. The new group appears in the list.

### Searching for a Group

To search for a group:

1. From the Administrator Configurator main menu, select **Group Configuration**. The Group Configuration screen opens. All currently-defined groups are listed.
2. Enter the name of the group in the Find dialog box and click **Find**. The group is selected in the list.

### Copying an Existing Group

To create a new group based on an existing one:

1. From the Administrator Configurator main menu, select **Group Configuration**. The Group Configuration screen opens, where all currently-defined groups appear in a list.
2. Select a group from the list and click **Copy**. The Group Properties screen opens with the properties of the copied group.
3. Give a new name to the group.

4. Change the settings, as needed.
5. When you are finished making changes, click **OK**. The Group Configuration screen re-opens.

### Modifying an Existing Group

To modify a group:

1. From the Administrator Configurator main menu, select **Group Configuration**. The Group Configuration screen opens, where all currently-defined groups appear in a list.
2. Select a group from the list and click **Change**. The Group Properties screen opens.
3. Make all changes as necessary and click **OK**. The Group Configuration screen re-opens.

### Deleting Groups

To delete a group:

1. From the Administrator Configurator main menu, select **Group Configuration**. The Group Configura-

tion screen opens, where all currently-defined groups appear in a list.

2. Select a group from the list and click **Remove**. The group should no longer appear in the list.

---

**NOTE:** *If you modify or delete a user's group, it doesn't change the user's profile.*

---

## Integrity Check

BOSÂNOVA Web supports profiles, which are definitions of host sessions. A profile is only active if it has been assigned to an existing host system. If that host system is then deleted from the Host Connection list, all profiles assigned to it become inactive.

To check for inactive profiles, run an integrity check.

1. From the Administrator Configurator, select **Integrity Check**. The Integrity Check screen opens.
2. Click **OK**. After several minutes, a list of all profiles currently assigned to invalid hosts is generated.
3. If needed, reactivate these profiles as follows:
  - a. From the Administrator Configurator, select **Session Configuration**. The Session Configuration screen opens.
  - b. Select one of the inactive profiles from the list and click **Change**. The Session Profile Properties screen opens.
  - c. In the **System Name** field, select an existing host connection from the list.
  - d. Click **OK** to save the changes. The Session Configuration screen re-opens. You can then select another inactive profile to reactivate by following steps b–d above.

## Server Monitor

Using the Server Monitor screen, the BOSÂNOVA Web System Administrator can create several reports:

- A report summarizing the configuration of the active BOSÂNOVA Web server
- A report describing active BOSÂNOVA Web sessions.
- Reports listing the content of the logs.
- A report listing all Help Requests.

In addition, the following two tasks are performed from the Server Monitor screen:

**Restarting** the BOSÂNOVA Web Server is performed from the Server Monitor screen. Restarting the server will disconnect all active connections.

**Stopping** the BOSÂNOVA Web Server is performed from the Server Monitor screen. Stopping the server will disconnect all active connections.

### Active Server's Configuration Report

To create a report summarizing the configuration of the active BOSÂNOVA Web server:

1. From the Administrator Configurator, select **Server Monitor**. The Server Monitor screen opens.
2. In the BOSÂNOVA Web server configuration summary field, click **Create a Report**. The report lists general information, HTTP Server configuration, Proxy Server configuration, and Server license configuration.

### Active Sessions Report

To create a report describing the sessions currently supported by the active server:

1. From the Administrator Configurator, select **Server Monitor**. The Server Monitor screen opens.
2. From the Session Report field, select the parameters for the report.
3. Click **Create a Report**. The Session Monitor screen opens with the completed report.
4. To change the sorting order of the Active Sessions report, select one of the sorting options from the report's header.
5. There are two ways to refresh the report:

- To refresh the report automatically, select **Refresh automatically every** and choose a time interval from the list.
- To refresh the report immediately, click **Refresh Now**.

### Disconnecting Sessions

You can disconnect sessions from the Session Monitor screen.

1. Create an Active Sessions report (see steps 1–3 in “Active Sessions Report” above).

2. Scroll down to **Disconnect options**.

3. Choose one of two disconnect options:

To disconnect individual sessions:

- a. Select **Select sessions to disconnect**.
- b. Select the checkbox to the left of a session.
- c. Click **Disconnect**. You can select more than one checkbox at a time.

To disconnect sets of sessions:

- a. Select **Disconnect all sessions with parameter**.
- b. Choose a parameter and a value from the two lists.
- c. Click **Disconnect**.

### Help Requests Report

To create a report listing all requests for Help submitted by Users

1. From the Administrator Configurator, select **Server Monitor**. The Server Monitor screen opens.
2. From the Log Reports field, click **Help requests**. A report listing all Help requests is displayed.

### Log Reports

A log file which reaches its size limit is saved to an archive. See *Log File Size* on p. 25

To view:

- Current log files, click either **Proxy log** or **HTTP log**.
- Archived log files, click **View old logs**.

### Server Update

Use the BOSâNOVA Web update utility to install BOSâNOVA Web server updates and to license BOSâNOVA Web.

#### Updating

An update is supplied by BOS either as a single zip-file or as a WEB location to download from.

---

***WARNING!*** Use only an update file and location that was produced by BOS.

---

1. From the Administrator Configurator, select **Server Update**. The BOSâNOVA Web Update Utility page is displayed.
2. Select an option for defining the location of the update file:

#### **Enter the address of the web site**

Select this option to download the update file from a location on the world-wide-web.

#### **Enter the local location**

Select this option if the update file is available on a local network or PC.



3. Click **Submit**. BOSâNOVA Web downloads the update zip-file to the server. The “Download completed” page is displayed.
4. Optionally, select **Backup** to create a copy of the server’s current configuration before the update overwrites it. The backup file is a compressed file which is created over the server’s backup directory.
5. Click **OK**.
6. A confirmation message is displayed. Click **OK** to continue. The “Extract completed” page is displayed.
7. Click **Apply** to complete the steps listed.
8. A confirmation message is displayed. Click **OK** to continue.

The final screen indicates if the server update completed successfully.

3. From the Administrator Configurator, select **Server Update**. The BOSâNOVA Web Update Utility page is displayed.
4. Select **License file**.
5. Enter the location of the license file and click **Submit**. A confirmation message is displayed informing you that the Server will restart. All active sessions will be disconnected.
6. Click **Submit**.

## Licensing

To license an installation of BOSâNOVA Web:

1. Request the license file, via email, from BOS Technical Support. BOS Technical Support will send you the license file via email.
2. Save the license file on your computer and note where it was saved.

# **Customizing BOSâNOVA Web**

This section explains how to customize the BOSâNOVA Web log-in screen. It includes:

- “Overview” on page 62
- “Customizing the Appearance” on page 62
- “Customizing Functionality” on page 63

## Overview

The BOSâNOVA Web log-in screen can be customized.



Figure 2: Default Log-in Screen

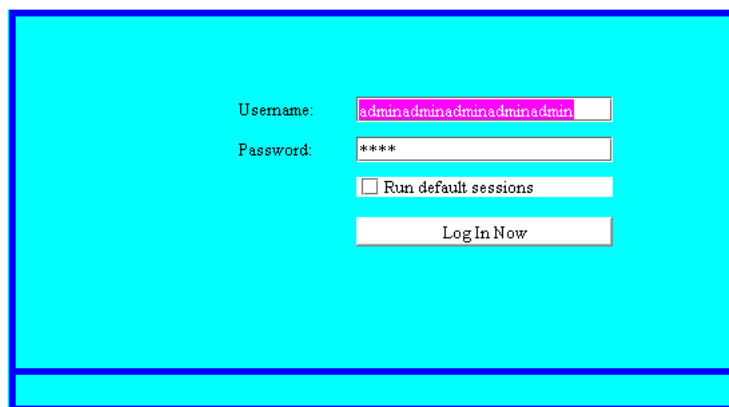


Figure 3: Sample Customized Log-in Screen

## Customizing the Appearance

The background image, and the colors of texts and fields of the log-in screen, can be customized.

### Customizing the Background Image

To change the background image:

1. Find the file named **BNWLOGIN.jpg**. It is located in the BOSâNOVA Web installation folder, in the folder named Images.
2. Change that file's name.
3. Copy the new background image into the Image folder.
4. Name the new background image **BNWLOGIN.jpg**.

### Customizing Colors

1. In the BOSâNOVA Web installation folder, find either the file named **NewFullClient.html** or **New-FullSSLClient.html**.

**NOTE:** This is the file that calls the applet. Optionally, you can change its name.

2. Make a copy of that file.
3. Using any standard text editor, open the original file.

4. Customize any or all of the following parameters:

---

**NOTE:** Define these colors using standard HTML hexadecimal values. Ensure that the symbol # precedes the value.

---

### **PANEL\_BACK**

This parameter determines the background color behind the Run default sessions field and the Log-in button. In Figure # 3, this is white.

### **SELECT\_BACK**

This parameter determines the background color behind the Username and Password when they are selected. In Figure # 3, these are magenta.

### **LABEL\_FORE**

This parameter determines the color of the texts. In Figure # 3, these are black.

### **STATUS\_FORE**

This parameter determines the color of the status prompt text that appears below the box. The prompt is not shown in Figure # 3.

### **STATUS\_BACK**

This parameter determines the background color of the status prompt text.

5. Save and close the file.
6. To view the changes, refresh the browser.

## Customizing Functionality

The applet can receive dynamic parameters through the HTML page which loads it. Use this feature to enable integration with external Web applications.

The dynamic applet parameters are loaded to the HTML by an external HTTP server and control the BOSâNOVA Web client functionality.

To customize functionality:

1. In the BOSâNOVA Web installation folder, find either the file named `NewFullClient.html` or `New-FullSSLClient.html`.

---

**NOTE:** This is the file that calls the applet. Optionally, you can change its name.

---

2. Make a copy of that file.
3. Using any standard text editor, open the original file.
4. Customize any or all of the following parameters:

### **USERID**

This parameter determines whether or not BOSâNOVA Web automatically displays the User ID. If left empty, the parameter is disabled. If a session name was set to include characters of the user name, this parameter is used to create the session name. This is applicable, as well, when log-in is bypassed.

### **PASSWORD**

This parameter determines whether or not BOSâNOVA Web automatically enters the password. If left empty, the parameter is disabled.

### **RUNDEF**

When this parameter is defined as **YES**, BOSâNOVA Web selects the “Run default sessions” checkbox. When the user clicks Log-in, BOSâNOVA Web automatically runs the default sessions.

### **GUILANG**

This parameter determines the language used in the client User Interface. As of version 6.300, the available languages are English and Hebrew.

### **SSL**

This determines whether or not the applet should work via the Secure Socket Layer (SSL) and open secured connections.

### **GROUPID**

The applet works with the definitions of the Group, for example, the sessions associated with the Group and the log-in requirements. The ID entered here must be the same as the Group name entered on the Group Properties page (see “Group Name” on page 54).

---

**NOTE:** *The following two parameters function as a unit.*

---

These parameters override the Session name parameter described in step #4 of “Printer Session Profiles” on page 44. When configured, the log-in screen is skipped and the printer sessions run automatically.

Both the number of entries and the order of the entries must match.

### **PRT\_DEVICES**

This is a list of values, divided by the character ',' (comma).

### **PRT\_PROFILES**

This is a list of existing profiles, divided by the character ',' (comma).

Following is a correct example:

```
<PARAM NAME="PRT_DEVICES" VALUE="PRTAGEN01,PRTAGEN02">  
<PARAM NAME="PRT_PROFILES" VALUE="PRT01,PRT02">
```

The following example is incorrect:

```
<PARAM NAME="PRT_DEVICES" VALUE="PRTAGEN01">  
<PARAM NAME="PRT_PROFILES" VALUE="PRT01,PRT02">
```

5. Save and close the file.

# **Users Data Deployment**

This section contains information for users. It is the BOSâNOVA Web administrator's responsibility to provide this information to them along with their username and login information.

**Table 7: System Requirements for End-Users Computer**

	<b>Processor</b>	<b>OS</b>	<b>Memory</b>	<b>Java VM</b>	<b>Connection</b>
<b>PC</b>	Pentium 230 MHz or higher	Windows 95/98/ or Window NT/ 2000/XP	128 MB minimum	Sun Java Plug-in 1.4.1 and higher	TCP/IP
<b>Browser Requirements</b>	BOSâNOVA Web display and printer sessions run on the following browsers: <ul style="list-style-type: none"> <li>• Microsoft Internet Explorer, version 5 and higher</li> <li>• Netscape, version 6 and higher</li> <li>• Mozilla 1.3</li> </ul> <p><i><b>NOTE:</b> Ensure that the browser supports the Java 2 platform, Enterprise Edition™. Refer to the Computer Requirements listed above.</i></p>				

## Logging in Data

The BOSâNOVA Web administrator must provide the following log in data to the users:

- The IP address or Domain Name (DN) for the IBM iSeries or PC acting as the BOSâNOVA Web server.
- The Web server port number.
- A file (page) name is optional. When no file name is provided, the BOSâNOVA Web Client page opens. From the BOSâNOVA Web Client page the user can access sessions and the User Configurator.

For example:

To run sessions	<b>http://194.90.180.80:8080</b> IP address or DN    port
-----------------	--

For the User Configurator	<b>http://194.90.180.80:8080/User.html</b> IP address or DN    port    filename
To run sessions with SSL	<b>https://194.90.189.80:4443</b> IP address or DN    port
To run sessions via SSL with a user certificate	<b>https://194.90.189.80:4444</b> IP address or DN    port

## Enabling Automatic Login with MS Windows

BOSâNOVA Web can be configured to automatically enter the Windows User Name and password during login.

To enable the use of the Windows User Name, the System Administrator must add these two applet parameters to the server's LoginEmPri.html (or LoginEmPrSSLi.html) pages:

1. Add the parameter **WINUSER**:

When this parameter's value is **YES**, the Windows User Name becomes the user name in the BOSâNOVA Web login box.

2. Add the parameter **USERPASS**:



When this parameter's value is **YES**, the password used will be the same as the user name.

If both parameter values are **YES**, BOSâNOVA Web will attempt an automatic login.

# Firewall/Proxy Server Considerations

The BOSâNOVA Web Server may be located on your system in front of or behind a firewall and/or proxy server. Depending on your system configuration and the type of firewall or proxy server you have, you may need to reconfigure.

This section includes:

- Configuration if firewall provides only packet filtering, p. 69
- Configuration if firewall functions as a proxy server, p. 69

Configuration Examples:

- BOSâNOVA Web Server Behind Firewall/Proxy Server, p. 70
- Client Browser Behind Firewall/Proxy Server, p. 70
- BOSâNOVA Web Server & Client Browser Behind Firewall/Proxy Server, p. 71

## Firewall Provides Only Packet Filtering

If your firewall provides only packet filtering, you must:

- use legitimate Internet IP addresses
- enable communication for all ports listed below
- enable any IP restrictions, as necessary

**Table 8: Default Ports used by the Server**

Port	Intended For
3334	Incoming and outgoing connections with BOSâNOVA Web for Telnet sessions
7773	Incoming and outgoing connections with BOSâNOVA Web for Telnet sessions with SSL
4443	Incoming connections to built-in HTTPS server
8080	Incoming connections to built-in HTTP server
<p><b>NOTES:</b> These ports are all configurable. If you are using SSL with a user certificate, use port #4444 and configure exactly like it was port # 4443.</p>	

## Firewall Functions as a Proxy Server

If your firewall serves as a proxy server as well as providing packet filtering, see the configuration examples on the following pages, and set the parameters according to the example that most closely resembles your system configuration. All of the examples use the default BOSâNOVA Web port numbers.

The configuration examples are:

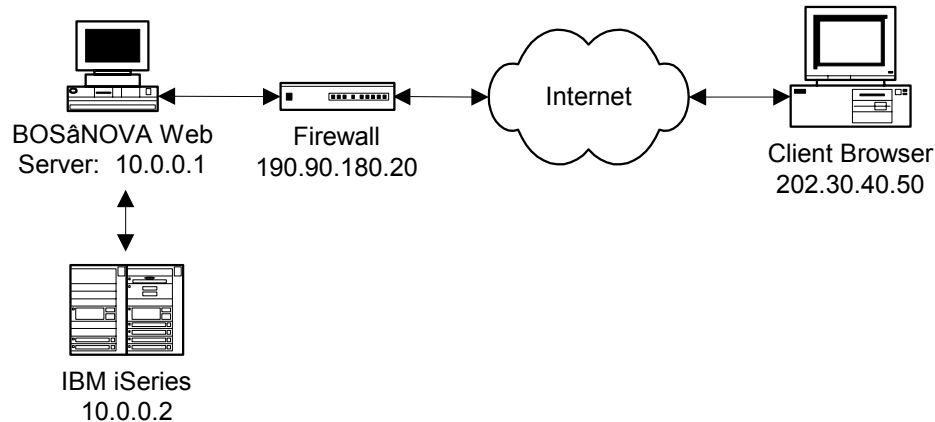
- “BOSâNOVA Web Server Behind Firewall/Proxy Server” on page 70
- “Client Browser Behind Firewall/Proxy Server” on page 70
- “BOSâNOVA Web Server and Client Browser Behind Firewall/Proxy Server” on page 71

If your firewall is acting as a proxy server only, you need:

- On the server side, IP re-mapping.
- On the client browser side, bypass the proxy server to the IP address of the BOSâNOVA Web server.

If this is not appropriate for your particular system configuration, contact BOS Technical Support for assistance.

### BOSâNOVA Web Server Behind Firewall/Proxy Server



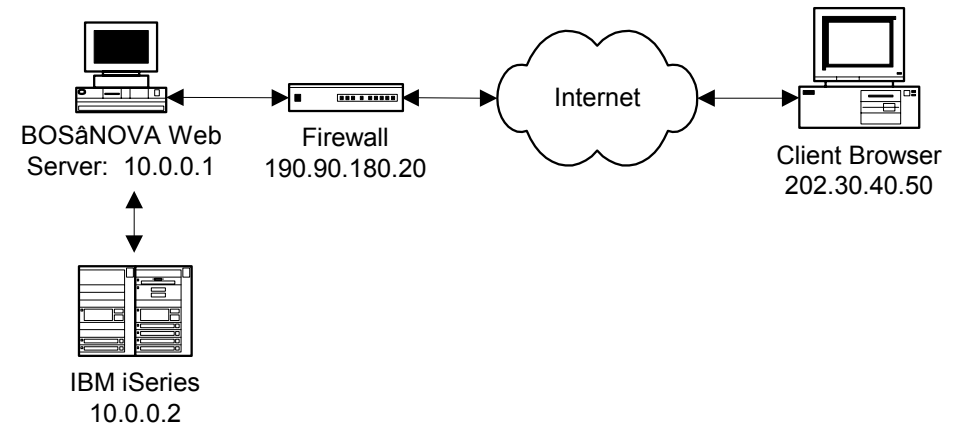
In this example, the client browser can't connect directly to the BOSâNOVA Web server, but must connect to the firewall (in this case, `http://190.90.180.20:8080/BOSâNOVA Web.htm`).

For this configuration, set the firewall parameters as follows:

- Enable incoming connections (from the Internet) to port 3334 and/or 7773 with re-mapping to address 10.0.0.1, port 3334 and/or 7773.
- Enable incoming connections (from the Internet) to port 4443 and/or 8080 with re-mapping to address 10.0.0.1, port 4443 and/or 8080.

- Enable outgoing messages/replies (to the Internet) from address 10.0.0.1, port 3334 and/or 7773 to any Internet host.
- Enable outgoing messages/replies (to the Internet) from address 10.0.0.1, port 4443 and/or 8080 to any Internet host.

### Client Browser Behind Firewall/Proxy Server



In this example, the client browser can connect directly to the BOSâNOVA Web server (in this case, `http://202.30.40.50:8080/BOSâNOVA Web.htm`).

For this configuration, set the firewall and client browser parameters as follows:

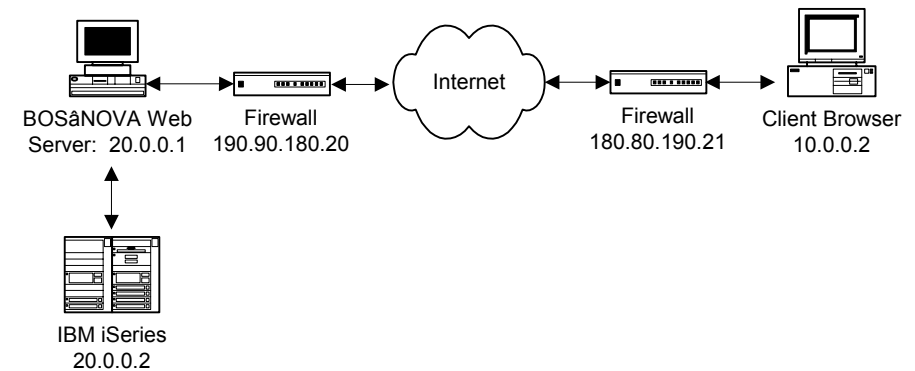
### Firewall

- Enable incoming messages/replies (from the Internet) from 202.30.40.50, port 3334 and/or 7773.
- Enable incoming messages/replies (from the Internet) from 202.30.40.50, port 4443 and/or 8080.
- Enable outgoing connections (to the Internet) to 202.30.40.50, port 3334 and/or 7773.

### Client Browser

Configure the browser to bypass the proxy server for address 202.30.40.50.

## BOSâNOVA Web Server and Client Browser Behind Firewall/Proxy Server



In this example, the client browser can't connect directly to the BOSâNOVA Web server, but must connect to the server-side firewall (in this case, [http://190.90.180.20:8080/BOSâNOVA Web.htm](http://190.90.180.20:8080/BOSâNOVAWeb.htm)).

In this example, the firewall and client browser parameters are set as follows:

### Server-side Firewall

- Enable incoming connections (from the Internet) to port 3334 and/or 7773 with re-mapping to address 20.0.0.1, port 3334 and/or 7773.
- Enable incoming connections (from the Internet) to port 4443 and/or 8080 with re-mapping to address 20.0.0.1 port 4443 and/or 8080.

## **BOSâNOVA Web Administrator Guide**

- Enable outgoing messages/replies (to the Internet) from address 20.0.0.1, port 3334 and/or 7773 to any Internet host.
- Enable outgoing messages/replies (to the Internet) from address 20.0.0.1, port 4443 and/or 8080 to any Internet host.

### **Client Browser**

Configure the browser to bypass the proxy server for address 190.90.180.20.

### **Client-side Firewall**

- Enable incoming connections (from the Internet) from 190.90.180.20, port 3334 and/or 7773.
- Enable incoming connections (from the Internet) from 190.90.180.20, port 4443 and/or 8080.
- Enable outgoing connections (to the Internet) to 190.90.180.20, port 3334 and/or 7773.

# SSL Configuration

This appendix includes:

- Understanding the Need for SSL, p. 74
- Public Key Encryption, p. 74
- One-way Hash Functions, p. 75
- Digital Signatures, p. 75
- Symmetric Cryptography, p. 76
- Authentication, p. 76
- Understanding How SSL Works, p. 78

## The Need for SSL

There are three problems you might encounter when you send information over the Internet or Intranet:

- **Eavesdropping**, where your information remains intact, but its privacy is compromised.
- **Modification**, where your original information is changed or replaced and then sent to the recipient.
- **Impersonation**, where your information passes to a person who poses as the intended recipient. This type of impersonation is known as *spoofing*.

The Secure Sockets Layer (SSL) protocol provides several features that safeguard against these threats.

- **Confidentiality** is guaranteed through encryption (see *Public Key Encryption* on page 74).
- **Integrity** is also ensured through encryption and special check sums (hashes) that are provided with each message (see *One-way Hash Functions* on page 75).
- **Authentication** is provided through digital signatures, which are very difficult to falsify (see *Digital Signatures* on page 75).

## Public Key Encryption

In public key encryption, two keys are used: One for encrypting data and the other for decrypting. The encryption key is called the public key and the decryption key is the private key. Anyone with the public key can encrypt a message but not decrypt it. Only the person with the private key can decrypt the message.

Here is an example describing how two stations can communicate using public key cryptography:

1. Station A generates two keys, a public key and a private key.
2. Station B generates two keys, a public key and a private key.
3. Both stations exchange their public keys.
4. Station B uses station A's public key to encrypt data that must be sent to station A, and station A uses its private key to decrypt data received from station B.
5. Station A uses station B's public key to encrypt data that must be sent to station B, and station B uses its private key to decrypt data received from station A.

Note that public keys are exchanged openly, without any encryption. As long as you do not share your private key, your encrypted messages are safe from tampering. Even an eavesdropper who gets both the public key and the ciphertext can't discover your private key or your original message.



There are several methods of public/private key pair generation. The most popular methods are RSA and DH (Diffie-Hellman).

### One-way Hash Functions

A one-way hash function or message digest is a digital fingerprint of a message, derived by applying a mathematical algorithm on a variable-length message. There are several suitable algorithms, each having the following special properties:

- The original message (the input) is of variable length.
- The message digest (the output) is of fixed length.
- It is practically impossible to determinate the original message (the input) from just the message digest (the output). This is known as a one-way hash function.
- It is practically impossible to find two different messages (the inputs) that create the same message digest (the output).
- The algorithm is relatively simple, so when computerized it is not CPU-intensive.
- The calculated digest is smaller than the item it represents.

The message digests are used to guarantee that no one has tampered with a message during its transit over a network.

The most common one-way hash function algorithms are MD5 and SHA1.

### Digital Signatures

Digital signatures involve swapping the role of the private and public keys. That is, if a sender encrypts a message using the sender's private key, everyone can decrypt the message using the sender's public key. A successful decryption implies that the sender, who is the only person in possession of the private key, must have sent the message.

This also prevents repudiation, that is, the sender cannot claim that he or she did not actually send the message. A piece of data encrypted with a private key is called a digital signature. Common practice is to use a message digest as the item of data to be encrypted.

## Symmetric Cryptography

In symmetric cryptography, the encryption algorithm requires the same secret key to be used for both encryption and decryption.

The advantage of these algorithms is that they are fast and efficient. They are generally at least 1000 times faster than public key algorithms. However, the problem is that of key exchange, the mechanism for safely ensuring that both parties, the sender and the receiver, have the secret key. This is one of the weakest areas of symmetric cryptography. How do you send the key to partners? You cannot just send it in an email message, because it could be intercepted and, possibly, compromise your security. So, the common practice is to exchange a secret key using the public key encryption at the first stage of communication and then use a symmetric cipher for session data encryption.

The best known symmetric encryption algorithms are RC2, RC4, and DES.

## Authentication

Over the Internet/Intranet, authentication takes the form of a digital certificate, or simply, a certificate. Both clients and servers can have certificates. When a server sends its certificate to a client, the process is called *server authentication*. When a client sends a certificate to a server, the process is called *client authentication*.

A certificate is an item of information that binds the details of an individual or organization to their public key. The certificate is signed with the Certificate Authority's (CA) private key to guarantee its authenticity and integrity. A CA is a third party, trusted by both communicating parties, that is responsible for both the contents and ownership of a certificate. There are several well-known CA companies including VeriSign, Inc. and Thawte, Ltd.

A certificate consists of the following parts:

Part Name	Description
Version	Identifies the certificate format.
Serial number	A value unique to the CA.
Algorithm identifier	Identifies the algorithm used to sign the certificate, together with any necessary parameters.

Part Name	Description
Issuer	The name of the CA.
Period of validity	A pair of dates. The certificate is valid during the time period between the two.
Subject	The name of the client or server.
Subject's public key	Contains the public key algorithm name, any necessary parameters, and the public key.
Signature	The CA's signature.

A certificate where the Issuer and Subject are the same is called a self-signed or root certificate. Usually such self-signed certificates are used for deploying CA private keys. Every Internet browser contains a set of self-signed certificates of the most popular CAs. If you are using Microsoft

Internet Explorer, then you can review them at Tools >Internet Options > Content > Certificates.

When an Internet browser (client) connects to an SSL-enabled Web server, then the server authentication is accomplished with these steps:

1. The client requests a connection with an SSL-enabled server.
2. The server signs but doesn't encrypt its certificate and sends it to the client.
3. The client uses the server's public key, which is included in the certificate, to verify that the owner of the certificate is the same one that signed it.
4. The client checks whether the certificate's CA is one that it accepts. (In other words, the client looks in its CA certificate database for a certificate corresponding to the issuer of the server certificate.) If so, the client proceeds to the next step, otherwise, the client informs its user that an unknown CA issued this certificate.
5. The client compares the information in the certificate with the information it has about the server (e.g., if the URL is `http://www.company.com`, then `http://www.company.com` must be defined in the Common Name parameter of the Subject part of the certificate). If the information matches, the client accepts the site as authenticated.

## How SSL Works

The SSL protocol embraces all of the previously described technologies: public-key encryption, one-way hash functions, digital signatures, symmetric encryption, and authentication through the use of digital certificates.

An SSL connection is initiated by a client program (for example, an Internet browser) and then proceed as follows:

1. The client sends a request to connect to the secure server. For example, `https://www.company.com:4443`. This request contains a list of cipher suite names acceptable to the client. A cipher suite defines the type of symmetric cipher, the encryption key length, and a one-way hash function. For example, RC4 with 128-bit key and MD5 hash function.
2. The server chooses the strongest common cipher and sends a response that includes the selected cipher suite name along with the server pre-signed certificate. Optionally, this response may include a request for the client certificate.
3. The client checks if the server certificate was issued by a CA it trusts. If so, it proceeds to the next step. Otherwise, the client can cancel the connection or proceed without authentication.
4. The client compares the information in the certificate with the information it just received concerning the site: its domain name and its public key. If the information matches, the client accepts the site as authenticated.
5. Using the cipher, the client generates a session key (that is, a symmetric encryption key used only for this transaction) and encrypts it using the server's public key. If a request for the client certificate was received in step 2, then the client must send its certificate or respond with a *no certificate* message.
6. If the server receives a *no certificate* message from the client, the server immediately drops the connection. Otherwise, the server checks the client certificate and, if the server can accept the certificate, then it finishes setting up the SSL session.
7. The client and server use the session key to encrypt and decrypt the data they send and receive.

# Troubleshooting

This section includes:

- Starting the BOSâNOVA Web Server in Interactive Mode, p. 80
- Playing Back Trace Screens, p. 82
- Error Messages and Known Problems, p. 83
- Performance Issues, p. 86
- FAQs, p. 87

# Starting the Server in Interactive Mode

Use Interactive Mode to assist in troubleshooting.

If the installation process you chose did not create the Java programs—for example, if you performed certain Custom Installations via the IBM iSeries, or if you installed via a PC— create the Java programs before starting the BOSâNOVA Web server. If the installation process did create the Java programs, continue with *Starting in Interactive Mode*, p. 81.

---

**NOTE:** *The IBM iSeries operating system must support JDK 1.3. The following procedure is for versions V4R2 and higher. You must restart the BOSâNOVA Web server after every license change.*

---

## Creating Java Programs Before Starting the Server

To create the Java programs:

1. Make sure that TCP/IP is started on the IBM iSeries.
2. Open a display session and log on to the IBM iSeries server.

---

**NOTE:** *Creating the following programs may take up to 40 minutes.*

---

3. Create the first Java program. On the IBM iSeries command line, enter **CRTJVAPGM** and press **F4**.
4. In the screen that appears, enter the parameters that appear in bold and press **Enter**. (In the example below, bosanova\_web is the installation directory.)  
 Class file or JAR file: ..... /bosanova\_web/  
**iaik\*.jar**  
 Optimization: ..... 20  
 Replace program: ..... YES  
 Enable performance collection: .....NONE
5. Create the second Java program. On the IBM iSeries command line, enter **CRTJVAPGM** and press **F4**.
6. In the screen that appears, type the parameters that appear in bold and press **Enter**. (In the example below, bosanova\_web is the installation directory.)  
 Class file or JAR file: ..... /bosanova\_web/  
**servers.zip**  
 Optimization: ..... 20  
 Replace program: ..... YES  
 Enable performance collection: .....NONE
7. Create the third Java program. On the IBM iSeries command line, type **CRTJVAPGM** and press **F4**.

8. In the screen that appears, type the parameters that appear in bold and press **F10**. (in the example below, BOSâNOVA Web is the installation directory.)

```
Class file or JAR file:..... /jadvantage/  
bsjdvntg.zip  
Optimization:..... 20  
Replace program:..... YES  
Enable performance collection: ..... NONE
```

### Starting in Interactive Mode

To start in Interactive Mode:

1. Open a display session and log on to the IBM iSeries where BOSâNOVA Web is installed.
2. Make sure the IBM iSeries command line is at least two lines long. On the IBM iSeries command line, type **CHGCURDIR**, followed by the path and directory name where BOSâNOVA Web is installed, for example, **CHGCURDIR Jadvantage**, and press **Enter**.
3. Type **java** and press **Enter**.
4. Start the BOSâNOVA Web servers. Type the bold text exactly as it appears; note that it is **case-sensitive!**  
Class: **com.bos.Servers.RunServers**

5. Press **F10** to display the class program arguments and classpath lines. Type the BOSâNOVA Web directory in the classpath line.  
Parameters: ..... SN=<iSeries serial number>  
Classpath: ..... ./:./servers.zip:  
./iaik\_jce\_full.jar:./iaik\_ssl.jar:./  
bsjdvntg.zip

---

**NOTE:** The BOSâNOVA Web directory is too long for the field. Enter as much of the path as will fit. Place your cursor on the last letter, press **F10**, and then **Page Down**. Complete the path.

---

6. Complete:  
Classpath security check level: ..... **\*IGNORE**

# Playing Back Trace Screens

Technical Support might request that you play back the screens recorded during a trace. When the trace was recorded, an .scn file was created. You must open and run the .scn file. Follow this procedure:

1. With any text editor, open the file named "Jadvantage3\Users\- 2. Add these parameters:
  - Trace= <SCN file>
  - TraceMorph= 1
  - TraceCodePage=<code page class name>, for example: TraceCodePage = Cp500. The code page class name is listed in the SysLang.jtn file which is located at the server root directory.
- 3. Copy the .scn file to Jadvantage3\Traces directory.
- 4. Run BOSâNOVA Web. The only option displayed will be the .scn file.
- 5. Select the .scn file and click **Start**.
- 6. To advance through the screens of the recorded trace, use the keypad's right arrow key.

---

**NOTE:** The default value for the parameter `TraceCodePage=<code page class name>` is "Cp500" and is for English. The `<code page class name>` value can be changed for different languages. For example, the value for Hebrew is "Cp424". The parameter is case sensitive.

---



# Error Messages and Known Problems

If you received an error for which there is not enough information below to correct the problem, contact BOS Technical Support

Error	The client sent an invalid request.
Action	Contact BOS Technical Support.
Error	The evaluation period has expired.
Cause	Conditions of your license.
Action	Contact your BOS distributor to renew the license.
Error	You have exceeded the maximum number of users allowed.
Cause	Conditions of your license.
Action	Contact your BOS distributor to increase the number of users allowed.

Error	Received unknown completion code from the proxy.
Cause	Internal code.
Action	Try again. If the problem recurs, contact BOS Technical Support.
Error	Error reading files from the groups directory.
Cause	Directory or files may be corrupted.
Action	Try again. If problem recurs, contact BOS Technical Support.
Error	Error reading Servers.jtn file.
Cause	Connection to BOSâNOVA Web server port is not available.
Action	Contact your system administrator.
Error	Error reading files from the profiles directory.
Cause	Files may be corrupted.
Action	Try again. If problem recurs, contact BOS Technical Support.

Error	Error reading files from the users directory.
Cause	Files may be corrupted.
Action	Try again. If problem recurs, contact BOS Technical Support.
Error	Error during the creation of the new profiles configuration.
Cause	Encountered a problem while reconfiguring profiles during the update from an earlier version.
Action	Contact BOS Technical Support.
Error	Error while reading Syslang.jtn file.
Cause	Either a problem with the server or the file is corrupted.
Action	If you installed from the BOS CD-ROM, copy the Syslang.jtn file to the BOSâNOVA Web root directory on your server. If you installed BOSâNOVA Web from a download, you must obtain a new download and reinstall. If the problem persists, contact BOS Technical Support.

Error	Error in creation of the new BOSâNOVA Web configuration. Unable to rename the users directory.
Cause	Encountered a problem while reconfiguring BOSâNOVA Web during the update from an earlier version.
Action	Contact BOS Technical Support.
Error	Error in creation of the new BOSâNOVA Web configuration. Unable to read information from the User.jtn file.
Cause	Encountered a problem while reconfiguring BOSâNOVA Web during the update from the earlier version.
Action	Contact BOS Technical Support.
Error	User directory not found.
Cause	Directory may be corrupted.
Action	Contact BOS Technical Support.

Error	The Prtfonts.jtn file may be missing or corrupted. If you installed from the BOSâNOVA Web CD-ROM, this file is located in the BOSâNOVA Web folder in the BOSâNOVA Web directory of the BOS CD-ROM. Copy it to the BOSâNOVA Web root directory on your server. If you installed BOSâNOVA Web from a download, you must obtain a new download and reinstall.
Cause	As explained in the body of the message.
Action	If the reinstall does not work, contact BOS Technical Support.
Error	Some files could not be updated.
Cause	Due to a problem with the server, BOSâNOVA Web was unable to complete the Integrity Check.
Action	Correct the problem in the server and repeat the Integrity Check.
Error	The Hstprnt.lst file is missing.
Cause	As explained in the body of the message.

Action	If you installed from the BOS CD-ROM, this file is located in the BOSâNOVA Web folder in the BOSâNOVA Web directory of the BOS CD-ROM. Copy it to the BOSâNOVA Web root directory on your server. If you installed BOSâNOVA Web from a download, you must obtain a new download and reinstall. If the problem persists, contact BOS Technical Support.
Error	On IBM iSeries OS 5.1 and 5.2, cannot update server installation from a PC.
Cause	Known problem.
Action	Use Native Install to update the server.

## Performance Issues

Q1: What affects the speed of the BOSâNOVA Web loading process?

A1: Many parameters affect this; the main ones are the connection type and modem speed. In a local network, BOSâNOVA Web downloads in seconds. With Internet connections, download time depends on your ISP connection speed, Web throughput, and PC configuration.

Q2: It takes a long time for the BOSâNOVA Web server on the IBM iSeries to load. Why?

A2: This depends on your IBM iSeries configuration and resources. You can significantly improve the BOSâNOVA Web performance and reduce the IBM iSeries CPU consumption if you convert the BOSâNOVA Web server Java code into the IBM iSeries machine code before you run the BOSâNOVA Web server. After you have the Runs.inst save file restored on the IBM iSeries, you will be able to run the BNWCRT command. This is a CL program that converts the BOSâNOVA Web Java files into IBM iSeries native programs.

## FAQs


Q1: Which browsers can I use?

A1: You can use any browser that supports the Java 2 platform, Enterprise Edition™; for example, Microsoft IE v. 5 and higher or Netscape Navigator v.6 and higher.

Q2: On one PC, I ran many display and printer sessions without any problems. However, on another PC, I ran the same number of sessions and my browser hung up. Why?

A2: This depends on your PC and browser resources and configuration. You can run more sessions concurrently on PCs that are more powerful.

Q3: How do I change the printout configuration ( LPI ,CPI , page orientation, etc.)?

A3: When you start a printer session, the Printer Properties icon  will be shown in the Windows task bar. Right-click this button and select **Properties** to open Printer Session Properties. In the Page Setup tab, you can customize your printing parameters.

# Index and Navigation Tips

This section contains:

- “Using the Index” on page 89
- “Links to Index Headings” on page 89
- “Navigation Tips” on page 89
- “Index” on page 90

## Using the Index

All index entries are links. Place the cursor over any page number and the cursor will turn into a hand, similar to this:



Click the page number of the index entry and the focus will jump to the designated area of the document.

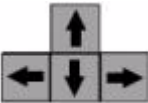
### Links to Index Headings

Use this table of Links to Index Headings to jump to entries beginning with a specific letter of the alphabet.

<b>A</b>	<b>B</b>	<b>C</b>	<b>D</b>	<b>E</b>
<b>F</b>	<b>G</b>	<b>H</b>	<b>I</b>	<b>J</b>
<b>K</b>	<b>L</b>	<b>M</b>	<b>N</b>	<b>O</b>
<b>P</b>	<b>Q</b>	<b>R</b>	<b>S</b>	<b>T</b>
<b>U</b>	<b>V</b>	<b>W</b>	<b>X</b>	<b>Y</b>
		<b>Z</b>		

## Navigation Tips

The following tips simplify navigation:

- To “turn the page” use either the right and left arrow keys or the up down arrow keys. 
- To display either the **Table of Contents** or the **Index**, click the links in the Navigation bar at the bottom of the page.
- **All page numbers are links.** Place the cursor over any page number and the cursor will turn into a hand. Click any page number and the focus will jump to the designated area of the document.
- Click **F4** to toggle **Bookmarks** in and out of view.
- **Bookmarks are links.** The cursor will turn into a hand. Click and the focus will jump to the Bookmark entry.
- To open the Find dialog box, click **Ctrl + F**.

# Index

## A

adding users .....	50
administrator configurator .....	23
access to .....	28
logging in .....	23
administrator troubleshooting .....	83
archives .....	59
AS/400	
configuring the system .....	12
creating Java program .....	80
import and export server setup .....	15
interactive mode .....	80
licensing .....	12
server requirements .....	6
starting interactive mode .....	81
starting server .....	80
startup during IPL .....	11
ASP .....	25
auto-reconnect timeout .....	27

## B

background customization .....	62
backing up server configuration .....	59

## C

clearing user configuration .....	53
client	
behind firewall/proxy server .....	70
color customization .....	62
configurator .....	23
configuring AS/400-based system .....	12
configuring groups	
copying .....	55
creating .....	54
deleting .....	56
modifying .....	56
searching .....	55
configuring host connections .....	38
configuring HTTP server .....	24
configuring proxy server .....	26
configuring sessions .....	40
defining a session name .....	48
display .....	41
printer .....	44
configuring SSL .....	29
configuring the server .....	24
configuring users .....	49
adding .....	50
copying existing user .....	52
deleting .....	52
modifying .....	52
connection timeout .....	27
copying	



display session profile .....	43	display session profiles .....	41
existing user configuration .....	52	copying .....	43
group .....	55	creating new .....	41
printer profile .....	47	deleting .....	43, 47
COR .....	45	modifying .....	43, 47
creating		<b>E</b>	
CSR .....	35	enable hot spots .....	42
groups .....	54	evaluation installation .....	6
new display session profile .....	41		
new printer session profile .....	44	<b>F</b>	
new SSL certificate folder .....	33	FAQs - Administrator .....	87
custom printer drivers .....	46	firewall/proxy server considerations .....	68
customizing		firewall/proxy server examples	
display emulation menus .....	44	behind firewall/proxy .....	70
log-in screen background .....	62	client behind firewall/proxy .....	70
log-in screen colors .....	62	server & client browser behind firewall/proxy .....	71
log-in screen functionality .....	63	firewall/proxy server types .....	69
<b>D</b>		free disk space .....	25
defining a new host connection .....	38	full installation .....	6
deleting		functionality customization .....	63
display session profile .....	43		
groups .....	56	<b>G</b>	
host connection .....	40	generating a user root certificate .....	33
printer session profile .....	47	global morph configuration .....	50
SSL certificate .....	38	graphic formats .....	26
users .....	52		
deleting objects .....	9	<b>H</b>	
disconnecting sessions .....	58	host connections .....	38

defining a new host .....	38
deleting .....	40
modifying .....	40
HTTP server configuration .....	24

## I

installing AS/400-based server	
from an AS/400's CD-ROM drive .....	6
installing PC-based server .....	16
integrity check .....	57
interactive mode	
creating Java program .....	80
starting server in .....	80
IPL startup .....	11

## K

keep alive session option .....	27, 39
---------------------------------	--------

## L

license information of active server .....	58
licensing AS/400-based system .....	12
licensing PC-based System .....	18
log file size .....	25
log reports .....	59
logging in	
configuring automatic .....	67
to the Administrator Configurator .....	23
using Windows settings .....	67
log-in screen customization .....	61

## M

menus customization .....	44
modifying	
existing host connection .....	40
existing user .....	52
group .....	56
printer profile .....	47
session profile .....	43
MorphMaster	
global morph configuration .....	50
setting in administrator's configurator .....	42

## N

NT service .....	17
------------------	----

## O

one-way hash functions .....	75
overwrite user's page parameters .....	45

## P

password, case sensitive .....	39
PC	
importing server setup .....	19
installing server .....	16
licensing .....	18
server installation prerequisites .....	16
server requirements .....	15
starting server .....	18
picture types .....	26

port numbers	
configuring .....	10
HTTP server default .....	25
Proxy server default .....	26
reapplying default .....	11
SSL default .....	26
printer drivers	
downloading custom drivers .....	46
overwriting user's driver .....	46
refreshing and resending .....	47
printer emulation	
overwriting user's parameters .....	45
printer session profiles .....	44
copying .....	47
creating a new .....	44
processor group license .....	13
proxy server configuration .....	26
public key encryption .....	74

## R

remote command server .....	39
remote program calls .....	39
remote stations, access to administrator configurator from .....	28
remove directory .....	8
restarting the server .....	57
ruler .....	42

## S

searching	
for a user .....	52
for groups .....	55
server	
monitor .....	57
restarting .....	57
security .....	28
stopping .....	57
updating .....	59
utilities .....	9
server & client browser behind firewall/proxy server ....	71
server behind firewall/proxy server .....	70
server configuration .....	24
importing from AS/400 .....	15
importing from PC .....	19
server reports	
active server configuration report .....	58
active sessions report .....	58
SSL .....	74, 78
authentication .....	76
digital signatures .....	75
how it works .....	78
one-way hash functions .....	75
public key encryption .....	74
symmetric cryptography .....	76
SSL certificates .....	32
changing .....	38
creating a new folder .....	33

creating a self-signed certificate .....	34
creating Certificates Signing Request (CSR) .....	35
deleting .....	38
generating a server SSL certificate .....	31
generating a user root .....	33
generating a user SSL certificate .....	31
installing server SSL certificate .....	31
installing user SSL certificate .....	31
viewing .....	38
SSL configuration .....	29
startall.log .....	18
starting	
AS/400 server .....	80
during AS/400 IPL .....	11
interactive mode .....	81
PC-based server .....	18
stopping the server .....	57

## T

trace screens .....	82
Troubleshooting	
administrator FAQs .....	87
performance issues .....	86
troubleshooting	
administrator .....	83

## U

uninstalling .....	8
uninstalling a PC-based server .....	20

updating the server .....	59
user	
adding new .....	50
clearing private configuration .....	53
importing from host .....	53
user configuration .....	49
users	
searching for .....	50
users data deployment	
logging in data .....	67
utilities .....	9

## W

working with SSL certificates .....	32
-------------------------------------	----