PageScope Enterprise Suite

Backup and Recovery

USER GUIDE

Date : 07/31/2008
Written by: Tony Gliatta, Vartkes Tashjian and Rob Posenato
Location: CEC Lab, HQ Ramsey, NJ

Table of Content

Introduction:

This guide has been created to discuss the Backup and Restore options of PageScope Enterprise Suite (PSES). PSES is a networked based server solution and necessitates the need for backing up stored data and restoring backed up data. This functionality is mandatory for surviving any possible system or network failures in order to maintain maximum server/application up-times.

In this guide we will discuss the Backup and Restore features of PSES. We will also provide step-by-step setup configurations to enable these features. Lastly we will discuss other industry standard backup & recovery methods and how these methods can be implemented in conjunction with PSES.

Document Scope:

PageScope Enterprise Suite Backup and Restore Procedure.

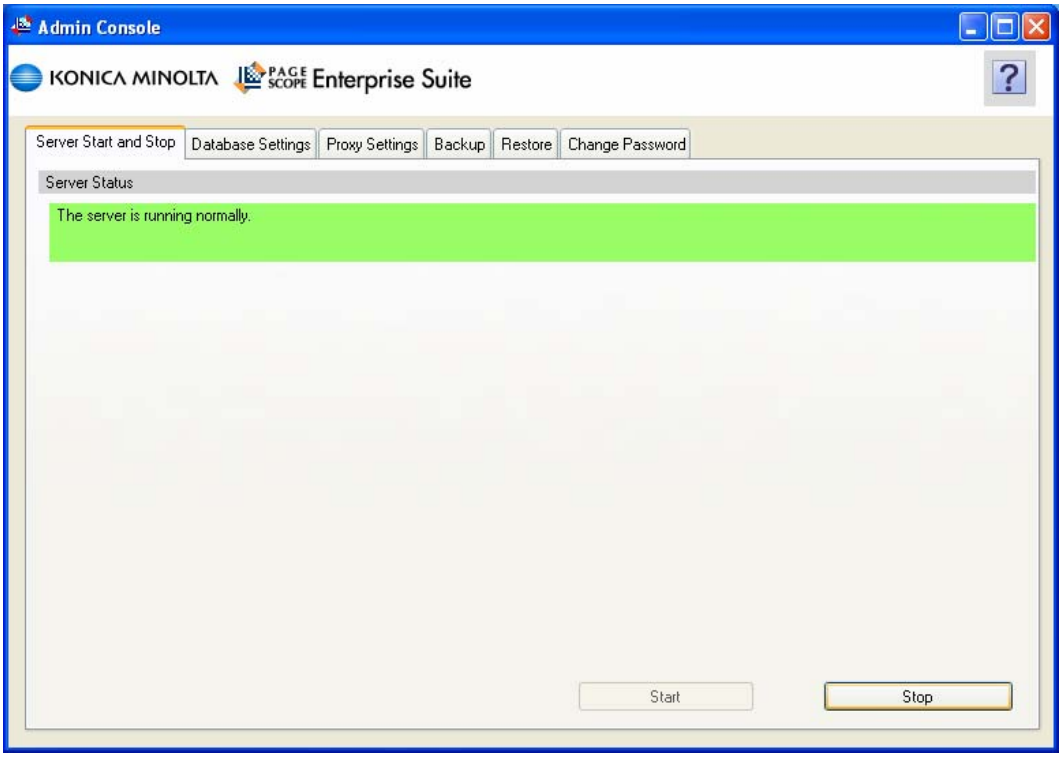
RAID Array

Chapter 1

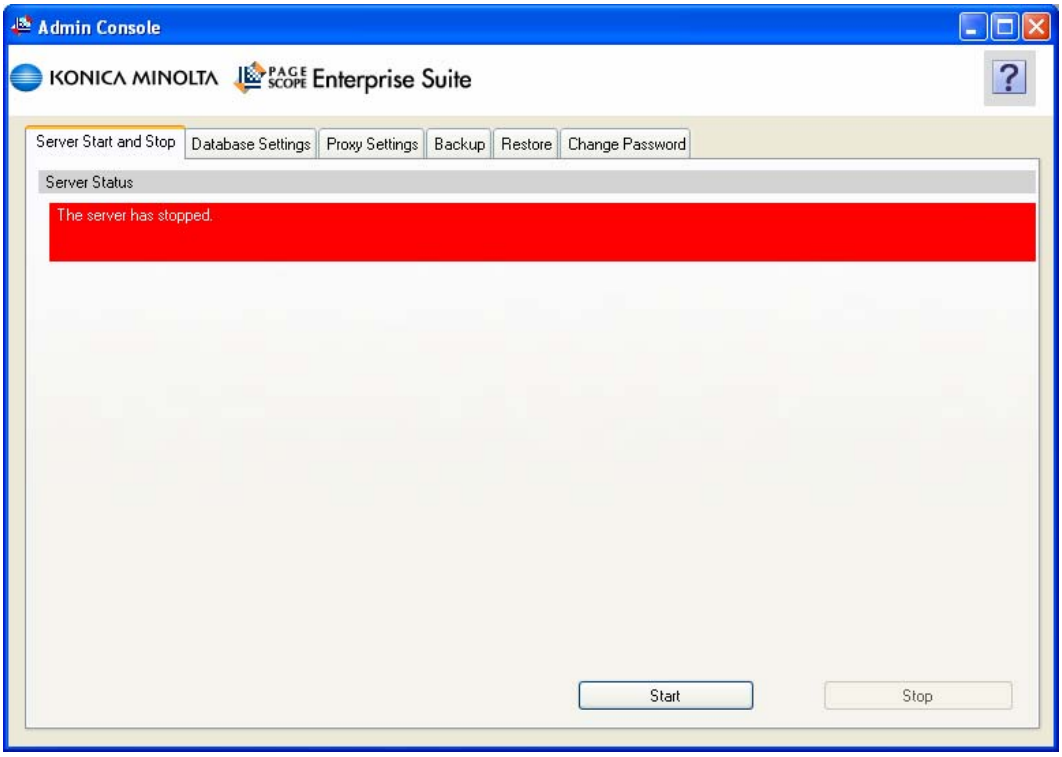
PageScope Enterprise Suite
Backup and Restore Procedure
(Local and/or network)

PageScope Enterprise Suite offers a Backup and a Restore feature built into the software application. This feature is designed to allow an IT administrator to backup the PSES database on a scheduled basis. This chapter will describe the step-by-step procedure involved for enabling and performing this operation.

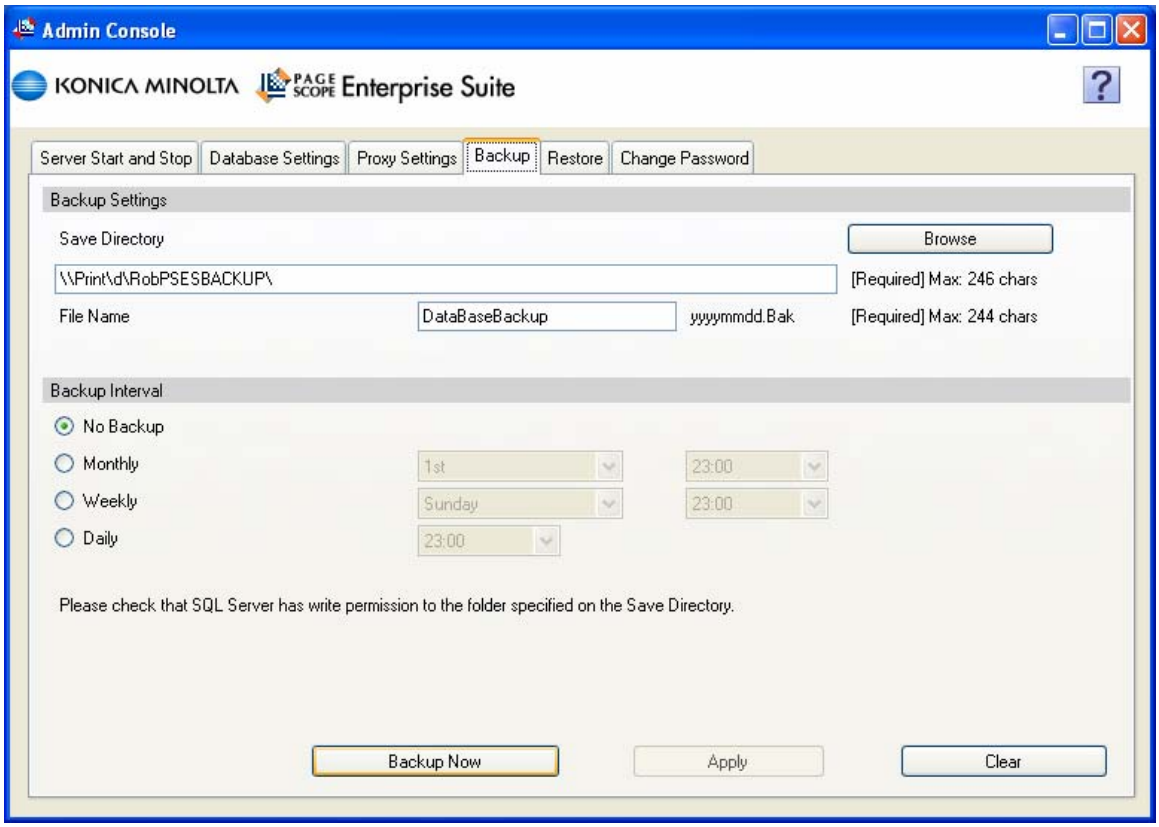
Creating a Database Backup:



Open the PSES Admin Console, and click the “Stop” button.



Once the server is stopped a message in red will display “The server has stopped.”



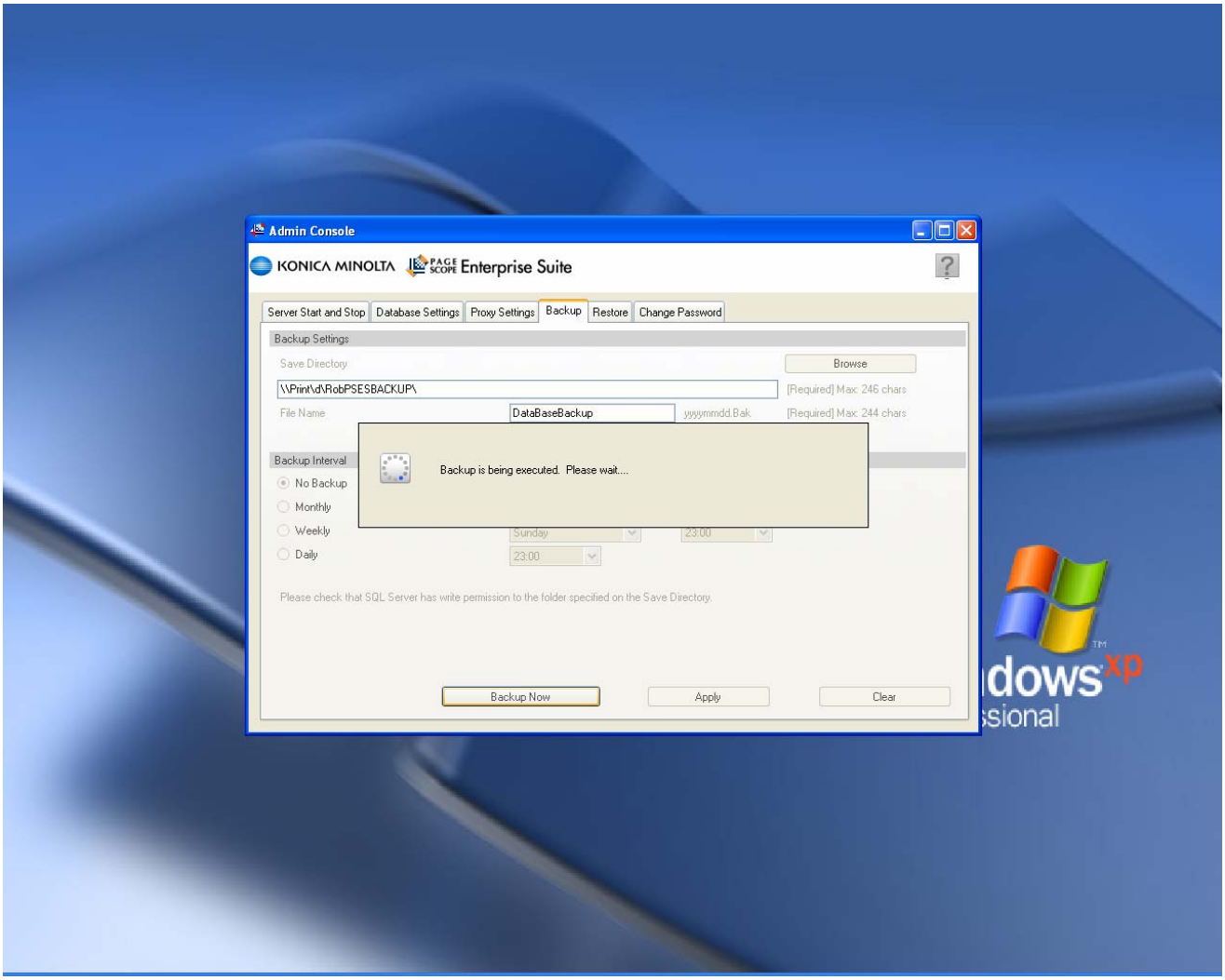
Next, click on the Backup Tab and select your destination folder by entering the local or network file path in the Save Directory field or clicking the Browse button and locating the intended folder.

Next enter a file name in the File Name field. Finally, an admin can schedule an automatic Backup Interval by selecting Monthly, Weekly, Daily and setting the appropriate day, date or time.

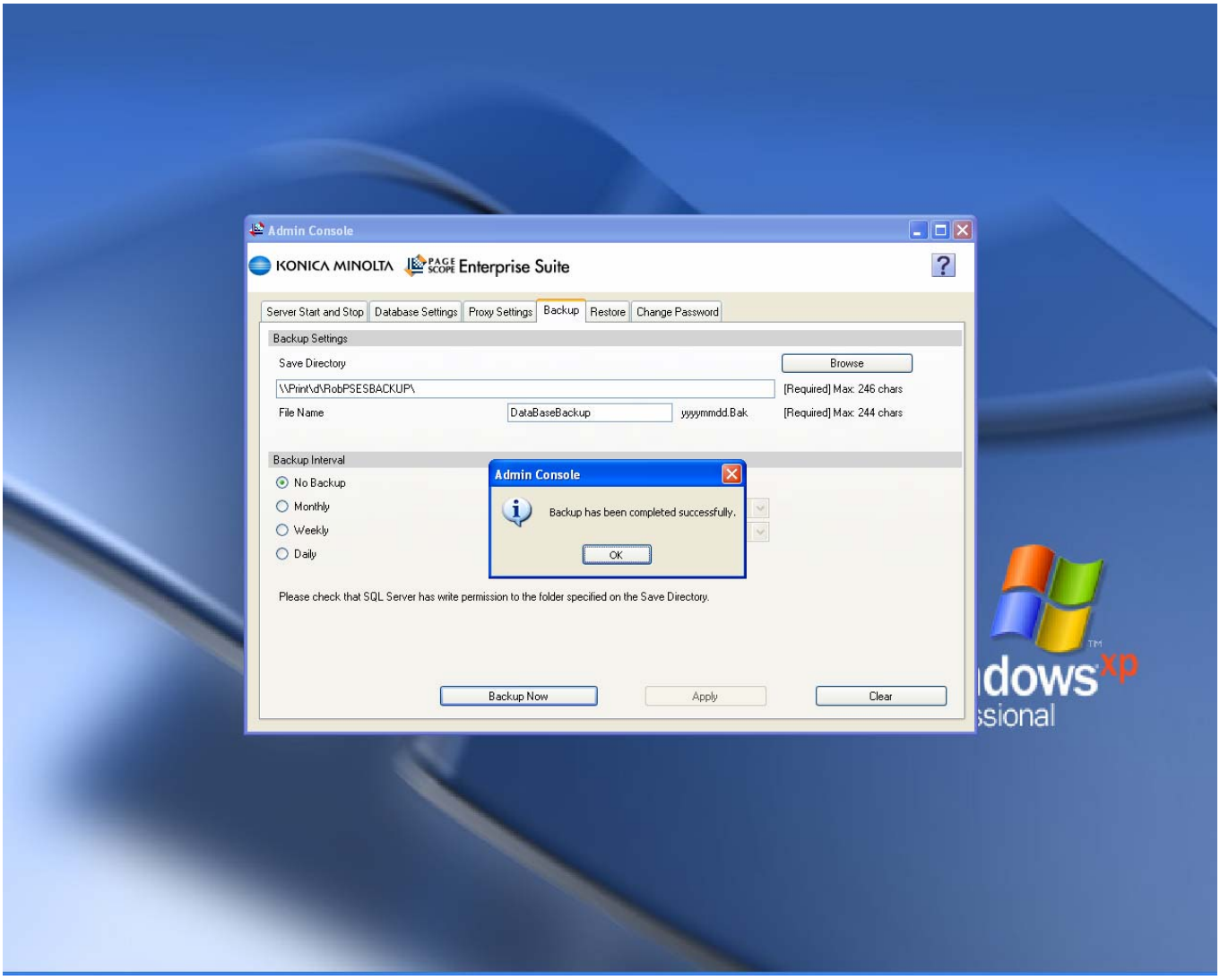
Click the apply button and select the “Backup Now” Button.

Note: When selecting a backup folder you MUST make sure that the User Group “SQLServer2005MSSQLUser$HOSTNAME$SQLPSESCORE” has FULL CONTROL of the selected folder otherwise it will not be able to create the backup.

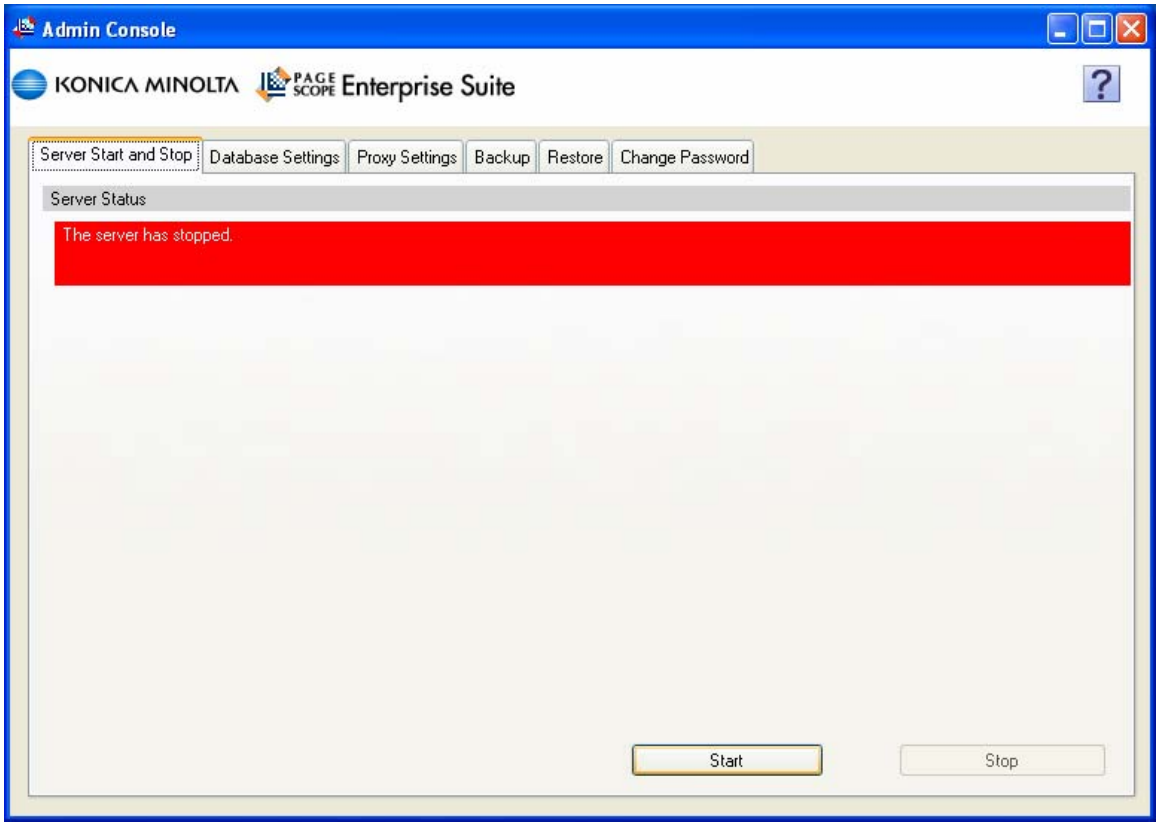
These permissions can be verified by right clicking on the intended folder, select properties, security tab.



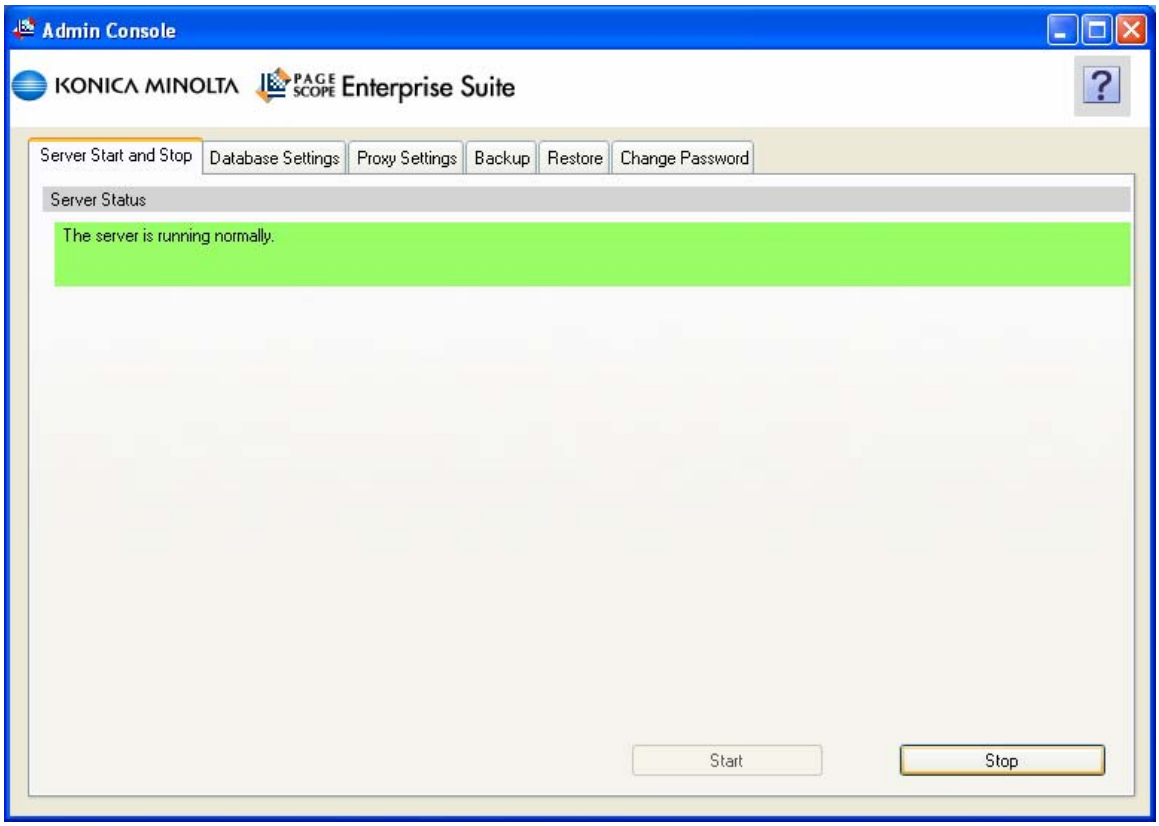
A “Backup is being executed. Please wait…” message is displayed during the backup process.



A “Backup has been completed successfully” window will open once the backup is done. To continue click the OK button.

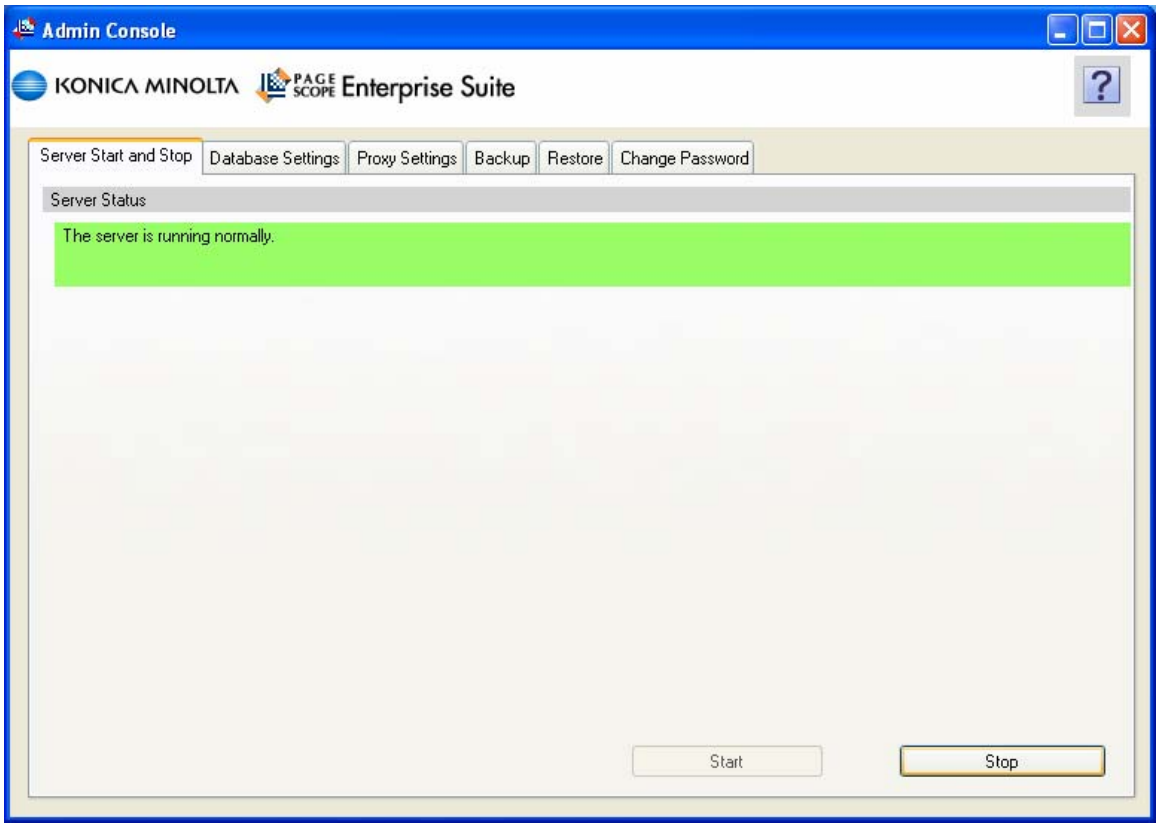


Navigate back to the “Server Start and Stop” tab and click on the “Start” button.

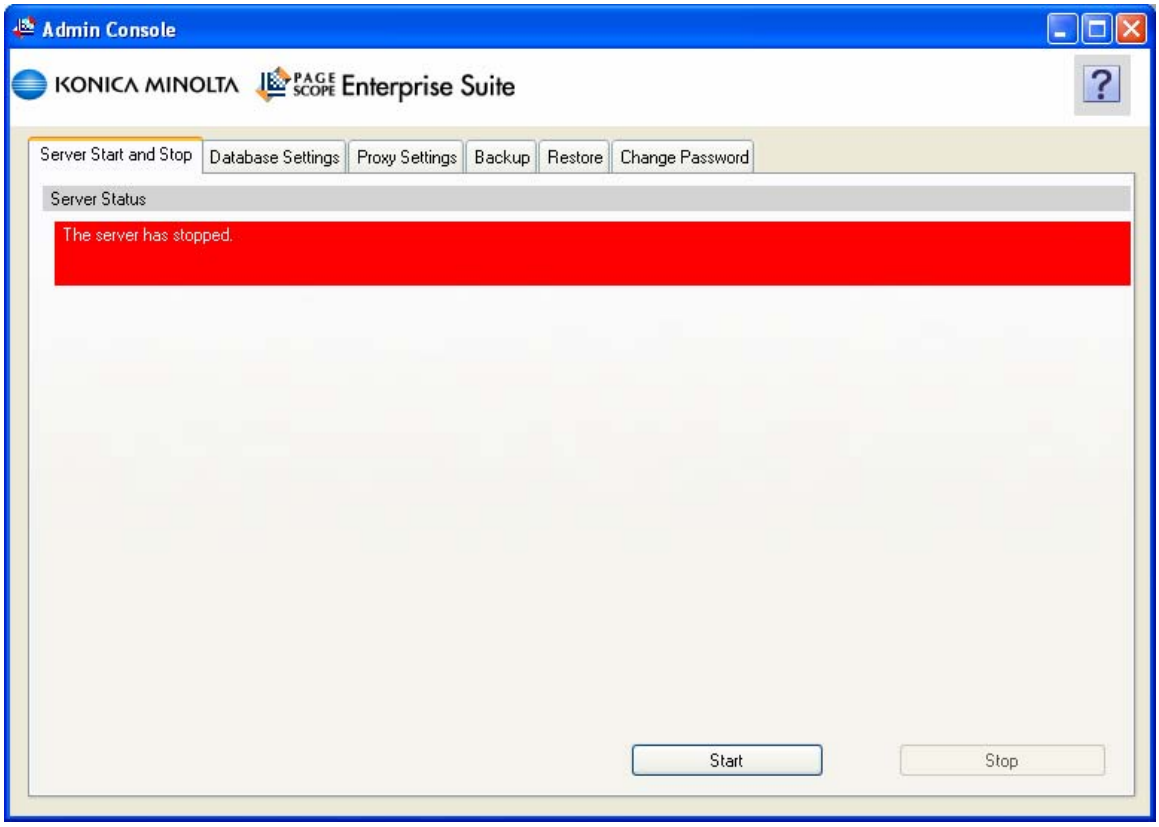


Once “The server is running normally.” is displayed the backup procedure of the database is complete.

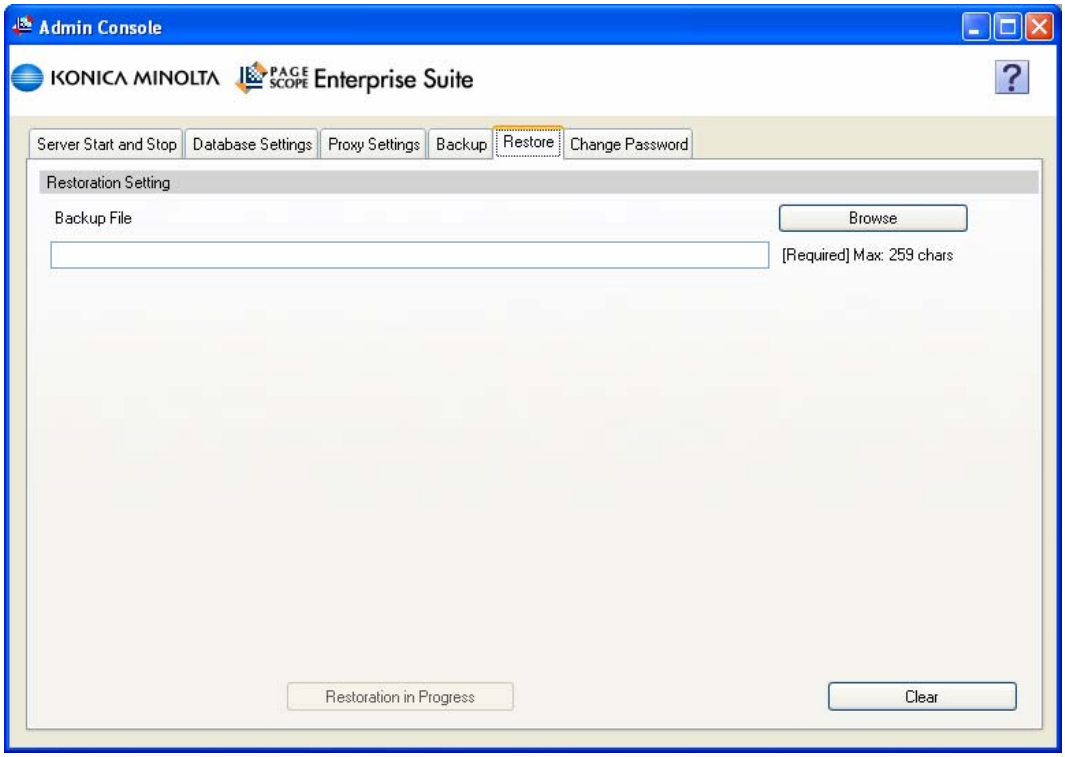
Restoring a Backup File:



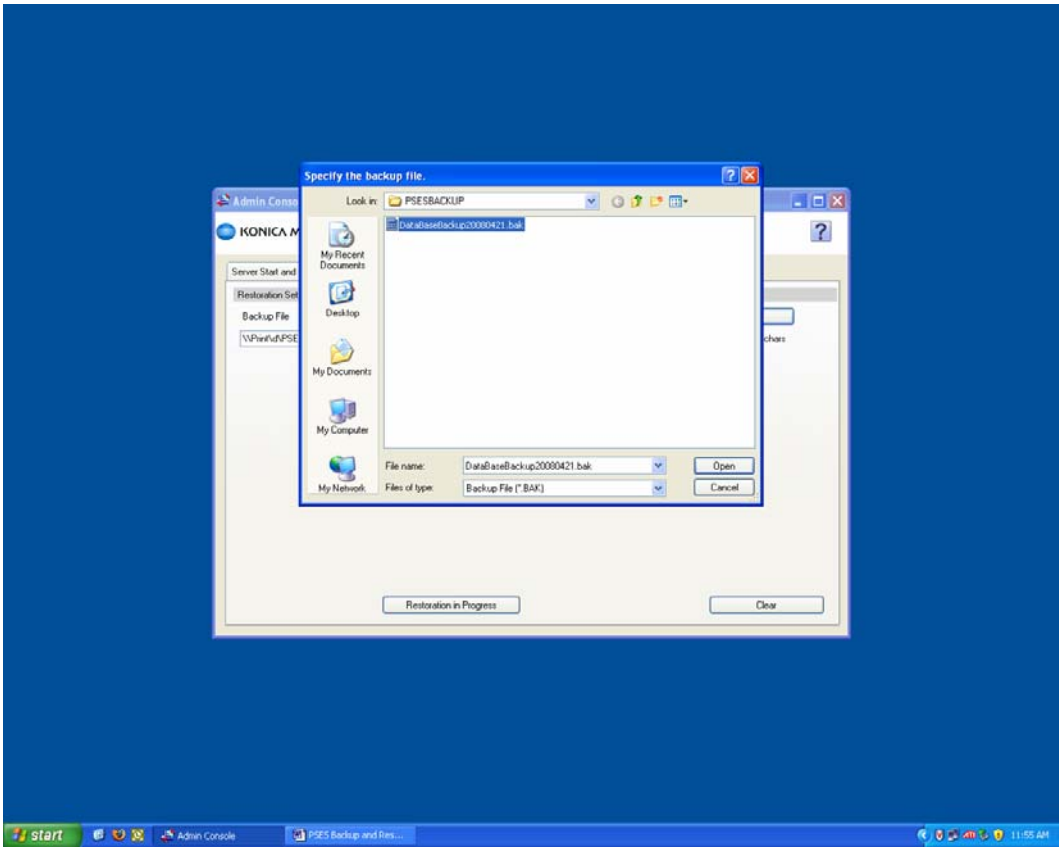
Open the PSES Admin Console, and click the “Stop” button.



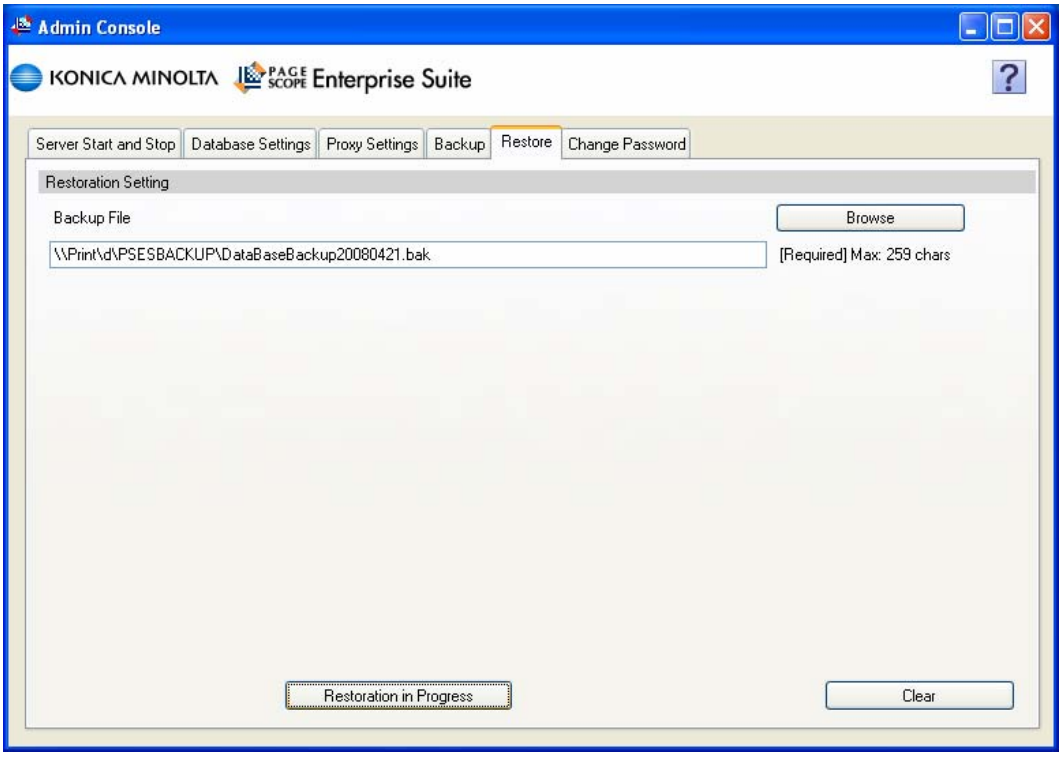
Once the server is stopped a message in the red will display “The server has stopped.”



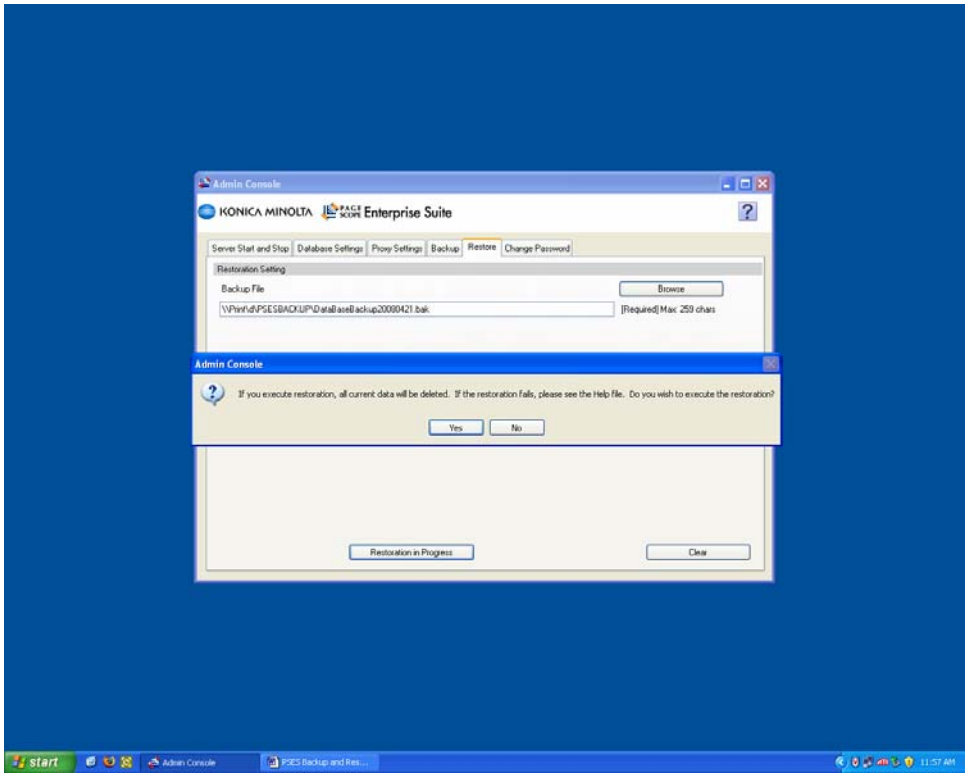
Click on the “Restore” tab, and then select the “Browse” button.



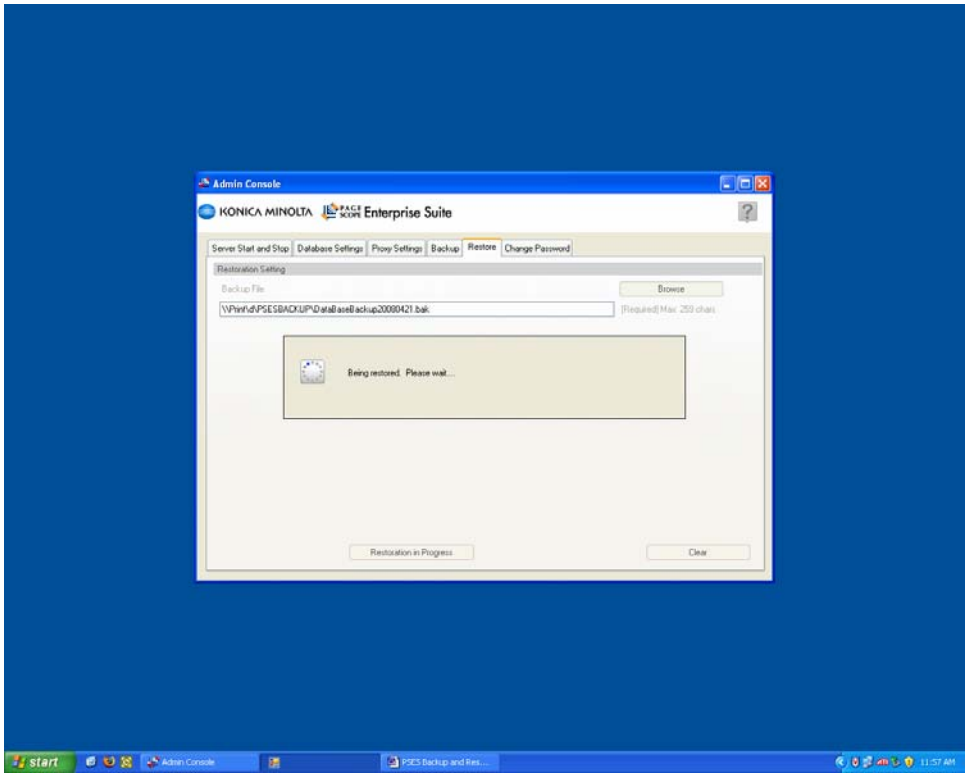
Navigate to the location where the database backup file is located (local or network location).
(See pages 5-9 to create a backup file)



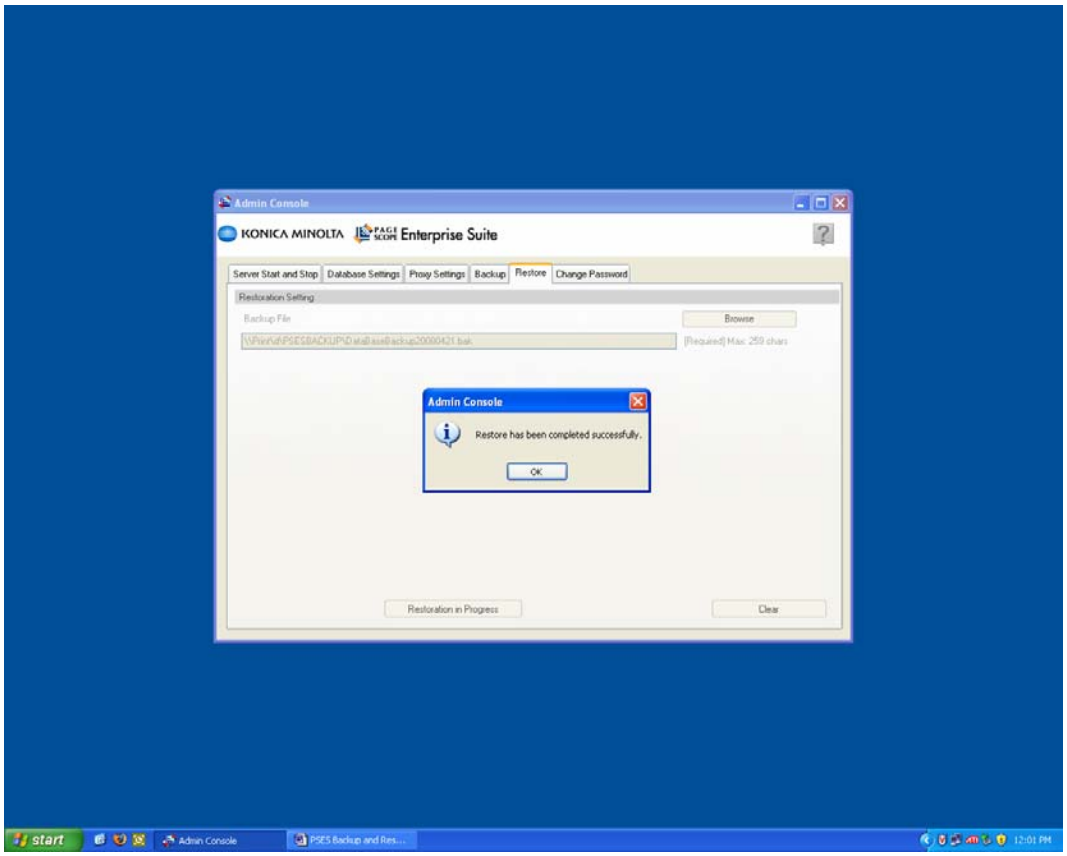
After selecting the backup file click on the “Restoration in Progress” button.



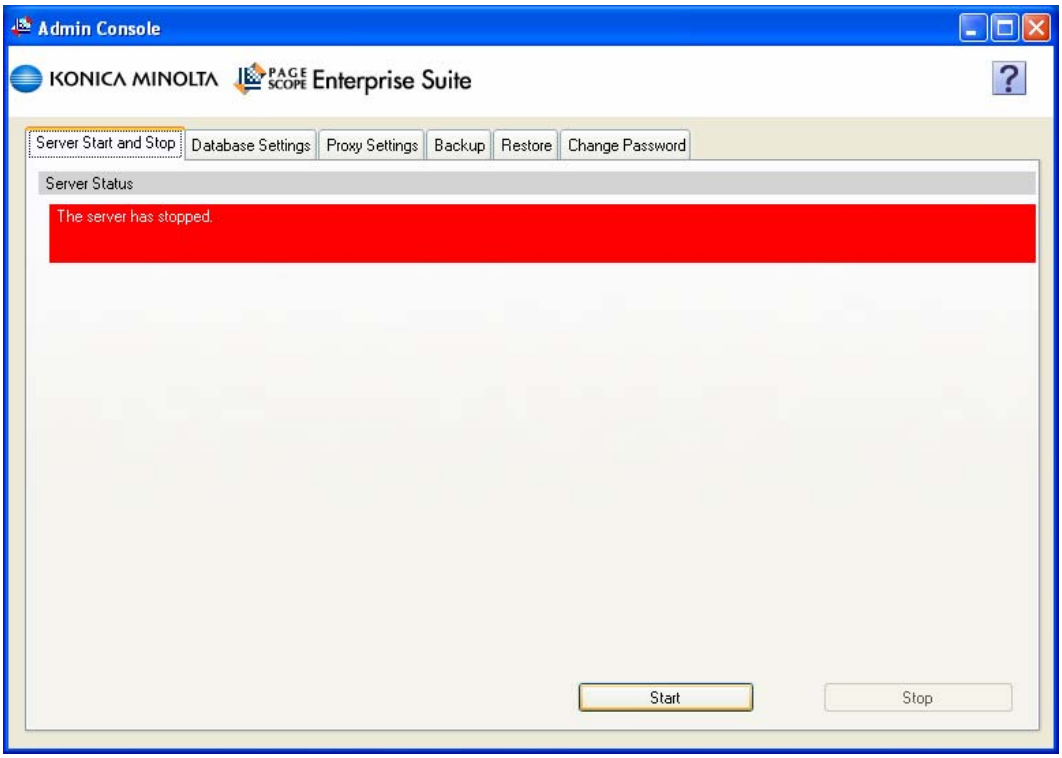
The next window will state “If you execute restoration, all current data will be deleted. If the restoration fails, please see the Help file. Do you wish to execute the restoration?” Click Yes to replace your data with the backup data.



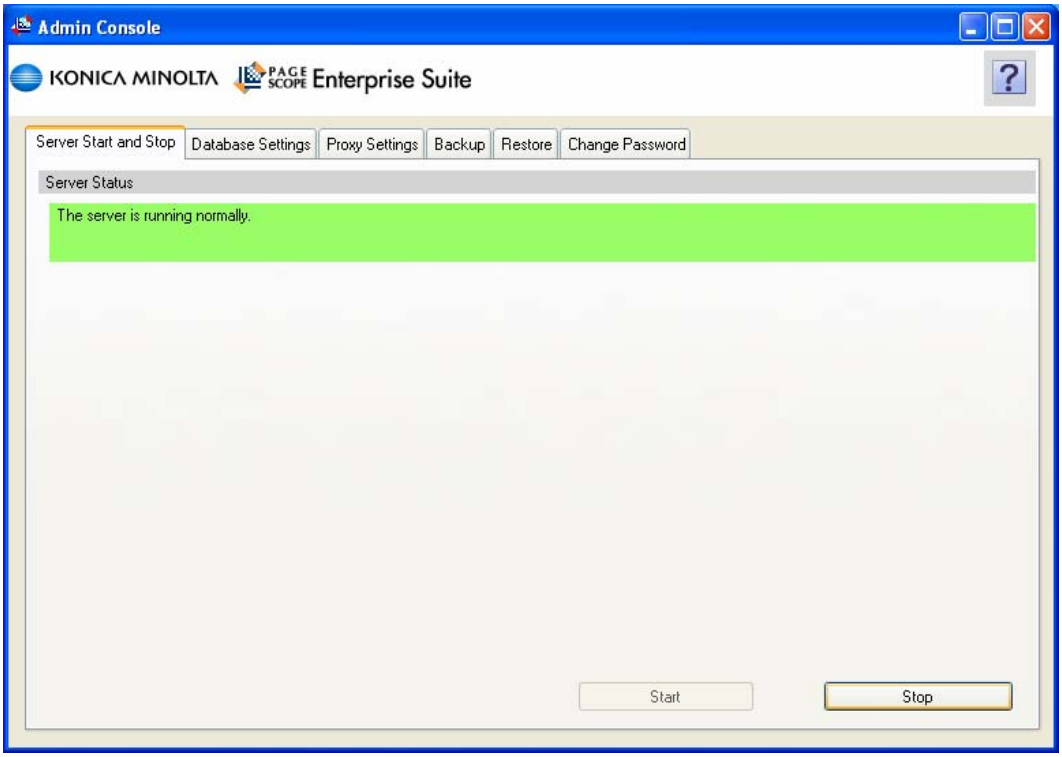
“Being restored, Please wait” is displayed. The database is being restored from the backup file.



When the restore is finished a new window will state “Restore has been completed successfully.” Click OK.



Navigate back to the “Server Start and Stop” tab and click on the “Start” button.



Once “The server is running normally.” is displayed the backup database restore process is complete.

Chapter 2

Recommended Industry Standard Practices

In this chapter we will discuss some of the Industry standard practices regarding backing up and storing critical data.

RAID Arrays

RAID — which stands for **Redundant Array of Independent Disks** — is a technology that employs the simultaneous use of two or more hard disk drives to achieve greater levels of performance, reliability, and/or larger data volume sizes.

The phrase "RAID" is an umbrella term for computer data storage schemes that can divide and replicate data among multiple hard disk drives. RAID's various designs all involve two key design goals: increased data reliability and increased input/output performance. When several physical disks are set up to use RAID technology, they are said to be *in* a *RAID* array. This array distributes data across several disks, but the array is seen by the computer user and operating system as one single disk. RAID can be set up to serve several different purposes, the most common of which are outlined below.

Purpose and basics

A RAID distributes data across several physical disks which look to the operating system and the user like a single disk. Several different arrangements are possible. We assume here that all the disks are of the same capacity, as is usual.

Some arrays are "redundant" in a way that writes extra data derived from the original data across the array organized so that the failure of one (sometimes more) disks in the array will not result in loss of data; the bad disk is replaced by a new one, and the data on it reconstructed from the remaining data and the extra data. A redundant array obviously allows less data to be stored; a 2-disk RAID 1 array loses half of its capacity, and a RAID 5 array with several disks loses the capacity of one disk.

Other RAIDs are arranged in a way that makes them faster to write to and read from than a single disk.

There are various combinations of these approaches giving different trade offs of protection against data loss, capacity, and speed. RAID levels 0, 1, and 5 are the most commonly found, and cover most requirements.

RAID 0 (striped disks) distributes data across several disks in a way which gives improved speed and full capacity, but all data on all disks will be lost if any one disk fails.

RAID 1 (mirrored disks) uses two (possibly more) disks which each store the same data, so that data is not lost so long as one disk survives. Total capacity of the array is just the capacity of a single disk. The failure of one drive, in the event of a hardware or software malfunction, does not increase the chance of a failure or decrease the reliability of the remaining drives (second, third, etc).

RAID 5 (striped disks with parity) combines three or more disks in a way that protects data against loss of any one disk; the storage capacity of the array is reduced by one disk. The less common RAID 6 can recover from the loss of two disks.

RAID involves significant computation when reading and writing information. With true hardware RAID the controller does the work. In other cases the operating system or simpler and less expensive

controllers require the host computer's processor to do the computing, which reduces the computer's performance on processor-intensive tasks (see "Software RAID" and "Fake RAID" below). Simpler RAID controllers may provide only levels 0 and 1, which require less processing.

RAID systems with redundancy continue working without interruption when one, or sometimes more, disks of the array fail, although they are vulnerable to further failures. When the bad disk is replaced by a new one the array is rebuilt while the system continues to operate normally. Some systems have to be shut down when removing or adding a drive; others support hot swapping, allowing drives to be replaced without powering down. RAID with hot-swap drives is often used in high availability systems, where it is important that the system keeps running as much of the time as possible.

It is important to note that RAID is not an alternative to backing up data. Data may become damaged or destroyed without harm to the drive(s) on which it is stored. For example, part of the data may be overwritten by a system malfunction; a file may be damaged or deleted by user error or malice and not noticed for days or weeks; and of course the entire array is at risk of catastrophes such as theft, flood, and fire [1].

[1] An excerpt from the internet definition website Wikipedia.com

Konica Minolta Business Solutions USA, Inc.
100 Williams Drive
Ramsey, NJ 07446
201-825-4000