Enterprise Suite
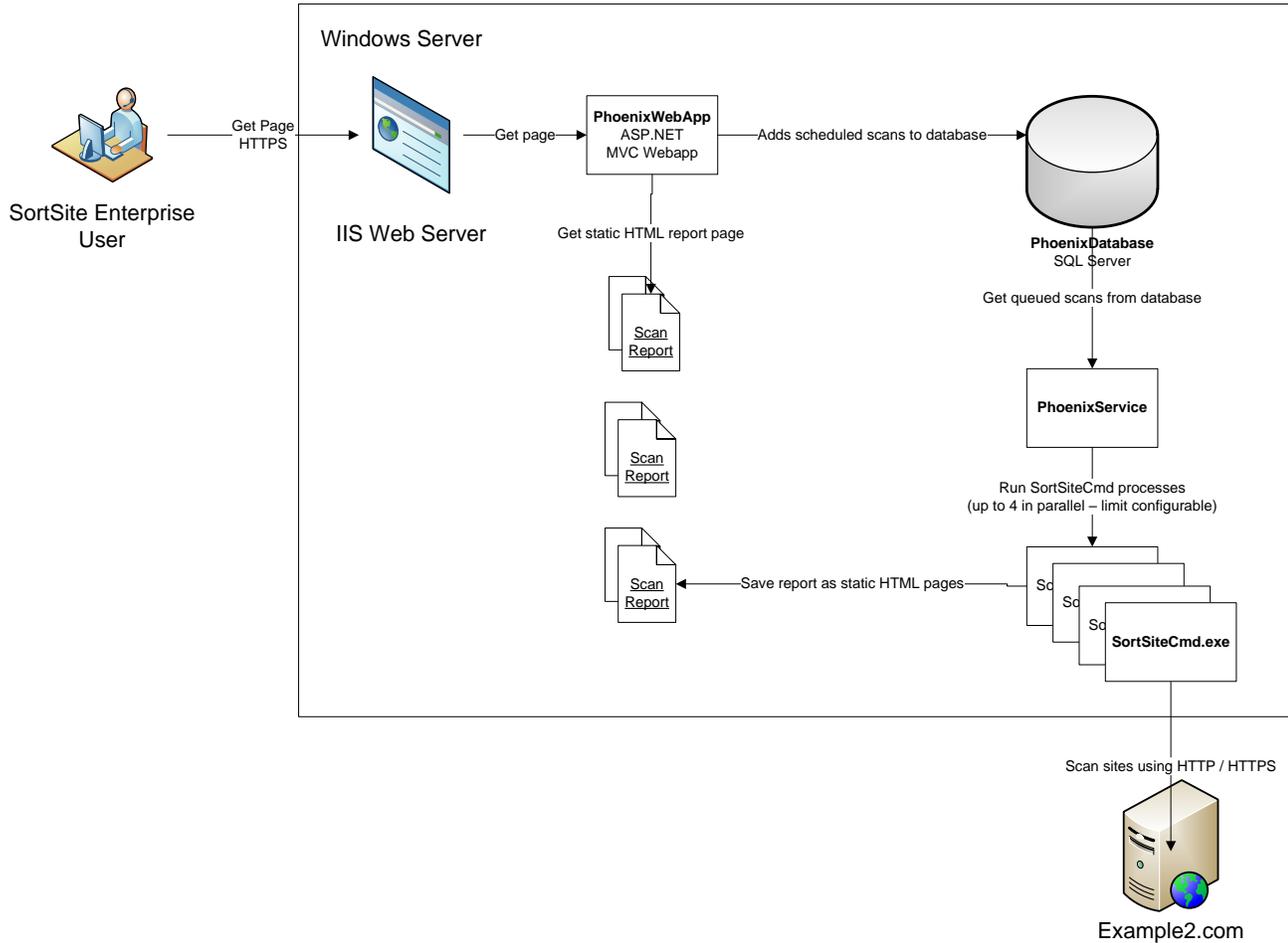Deployment Guide v2024.1.1

1 Introduction

This guide describes how to deploy Enterprise Suite and is intended for IT professionals. **Note:** Enterprise Suite was previously called SortSite Enterprise.

Enterprise Suite is a web application hosted on a Windows Server running IIS and SQL Server. You can use the web application from any device with a modern web browser (Windows, Mac, iPad, Android, Linux).

The simplest deployment option is hosting everything on a single server (either a physical server, or a virtual server instance running on a virtual machine).

Deployment consists of running a few installers with default options and changing a few configuration file entries. Once Windows is installed, installation can be done in under an hour by in-house IT staff.

2 Architecture

The basic architecture of Enterprise Suite is shown above. The main components are:

- **SortSiteCmd.exe** (aka CrawlerProcess) this is the scanning engine that performs website scans. Each scan runs as a separate process meaning scans cannot interfere with each other.
- **PhoenixWebApp** – provides the user interface to the system, used to manage scans and add scan requests to the scan queue
- **PhoenixService** – Windows service which polls the scan queue and starts an instance of SortSiteCmd.exe for each item pulled from the queue. Also sends email notifications and performs housekeeping.
- **PhoenixDatabase** – a SQL Server database containing lists of users, scheduled scans, and URLs of the scan results. The scan reports are static HTML files – this greatly reduces database size making the database much easier to backup and provides a lot of flexibility in storing the reports.

3 Recommended Hardware

The recommended configuration is a single server (or virtual machine instance) hosting all components. The database can be hosted on another server if required.

The server hardware requirements are fairly modest. The following is recommended for hosting on physical hardware:

- 64-bit dual core 2GHz CPU or better
- 4GB Ram or more
- 2 x 500GB disks (RAID1) or better

If hosting on a virtual machine, please refer to your vendor's documentation for hardware requirements required to provide an equivalent configuration.

Note: the hardware configuration above is used for OnDemand Suite (the SaaS version) and each server supports over 100 customers and more than 200 users scanning over 1 million pages per month.

If there are requirements for storing reports for long periods, we recommend increasing the disk storage. As with any server it's much cheaper and easier to add additional disk storage at the time a server is commissioned, but harder and more expensive to add once a server is live.

4 Performance Considerations

The web application is designed to impose a very low load on the server and is unlikely to be a bottleneck since reports are returned as static HTML pages.

Scanning speed is more likely to be an issue when scanning large sites (since number of pages impacts scanning speed). The most important factors affecting scanning performance are:

a) The size of the website being scanned affects scan duration. For example, if website A has 1,000 pages, and website B has 100,000 pages, then B will take 100x longer to scan than A (assuming both sites return pages at the same rate).

b) The rate that the websites being scanned return pages also affects scanning speed. For example, if website A takes 1 second to return a page, and website B takes 10 seconds to return a page then B will take 10x longer to scan than A (assuming both sites are the same size).

c) The network speed and latency between the SortSite Server and the websites being scanned also affects scanning speed. This is not a problem on most corporate networks unless the network is congested, or traffic management solutions are being used which throttle traffic.

5 Deployment

5.1 Required Information

You need the following information before you start:

- Name and port number of a mail server that can accept mail from the Enterprise Suite server (email is used for password resets and emailing scan results)

- Authentication details for SQL Server if you're hosting the database on a separate server (you don't need this for a local install of SQL Server)

5.2 Deployment Packages

The deployment packages used are:

Name	What	Update Frequency
CrawlerProcessFull.exe	Installs the MSI package for SortSiteCmd.exe (MSI can be extracted via command line option if required)	Quarterly – synched with SortSite maintenance releases. Updated to reflect updates to standards, fix false positives etc.
EnterpriseWebAppSetup.exe	Installs the MSI package for the web application component (MSI can be extracted via command line option if required)	Every 12 months approx
EnterpriseServiceSetup.exe	Installs the MSI package for Windows service (MSI can be extracted via command line option if required)	Every 12 months approx
PhoenixDatabaseInstall12.bacpac	Used to do a clean install of the database via SQL Server Management Studio.	Every 12 months approx

5.3 Platform Deployment - Windows Server 2016

One-time platform installation if hosting on Windows Server 2016:

1) Install Windows 2016 Server OS and connect to internal network

2) Login to the server via Remote Desktop or the console.

3) Using the Server Manager->Dashboard add the **Web Server (IIS)** role then add the **ASP.NET 4.8** feature under Role Services->Application Development

4) Using the Server Manager dashboard add the **SMTP Server** feature.

5) Install SQL Server (unless database is being hosted on another server or is already installed). SQL Server Express is a supported configuration. We

recommend installing SQL Server Management Studio to assist with configuration.

Important: the server collation should be SQL_Latin1_General_CP1_CI_AS (this is the default in most installations, but check before installing)

Note: Configuration files are pre-configured for the default SQL Express instance name "SQLEXPRESS"

6) To configure the Windows mail server for onward delivery:
a) Open IIS 6.0 Manager from the Administrative Tools folder in the Windows start menu
b) Open the SMTP Virtual server node, right click on Domains and select New Domain
c) Add a remote domain matching the part of your email address after the @ symbol (for example, enter agency.gov if your email address is john.smith@agency.gov)
d) Right click on SMTP Virtual server node and select Properties
e) On the Access tab click the Relay button and add 127.0.0.1 as the only server allowed to relay
f) Go the Windows Services administration console, set the Startup Type for the Simple Mail Transfer Protocol service to Automatic, and start the service

7) Install the ASP.NET Core hosting bundle https://learn.microsoft.com/en-us/aspnet/core/host-and-deploy/iis/hosting-bundle?view=aspnetcore-8.0

8) Run iisreset.exe at the command line

5.4 Platform Deployment - Windows Server 2019 or 2022

One-time platform installation if hosting on Windows Server 2019 or 2022:

1) Install Windows 2019 Server OS (with Desktop Experience) and connect to internal network (join domain at this point if required)

2) Login to the server via Remote Desktop or the console.

3) Using the Server Manager->Dashboard add the **Web Server (IIS)** role then add the **ASP.NET 4.8 Platform Deployment** feature under Role Services->Application Development

4) Using the Server Manager dashboard add the **SMTP Server** feature.

5) Install SQL Server (unless database is being hosted on another server or is already installed). SQL Server Express is a supported configuration. We recommend installing SQL Server Management Studio to assist with configuration.

Important: the server collation should be

SQL_Latin1_General_CP1_CI_AS (this is the default in most installations, but check before installing)

Note: Configuration files are pre-configured for the default SQL Express instance name "SQLEXPRESS"

6) To configure the Windows mail server for onward delivery:
a) Open IIS 6.0 Manager from the Administrative Tools folder in the Windows start menu
b) Open the SMTP Virtual server node, right click on Domains and select New Domain
c) Add a remote domain matching the part of your email address after the @ symbol (for example, enter agency.gov if your email address is john.smith@agency.gov)
d) Right click on SMTP Virtual server node and select Properties
e) On the Access tab click the Relay button and add 127.0.0.1 as the only server allowed to relay
f) Go the Windows Services administration console, set the Startup Type for the Simple Mail Transfer Protocol service to Automatic, and start the service

7) Install the ASP.NET Core hosting bundle https://learn.microsoft.com/en-us/aspnet/core/host-and-deploy/iis/hosting-bundle?view=aspnetcore-8.0

8) Run iisreset.exe at the command line

5.5 Initial Application Deployment

Once the base platform has been setup, the deployment process is:

1) Use the Import Data-tier Application command in SQL Server Manager Studio to install the database from the .bacpac file. After import create the following SQL Server users

    [NT Authority/Local Service] – default database Phoenix, and assign to the roles: PhoenixServiceRole, db_datawriter, db_datareader
    [NT Authority/Network Service] default database Phoenix, and assign to the roles PhoenixWebRole, db_datawriter, db_datareader

2) Run EnterpriseWebAppSetup.exe and install to default location

3) Run CrawlerProcessFull.exe and install to default location

4) Run EnterpriseServiceSetup.exe and install to default location

5) Change the database connection strings in ConnectionStrings.instance.config and appsettings.Production.json as follows:

    • If you've installed SQL Server Express using the default instance name of .\SQLEXPRESS then no changes are needed

- If you've installed any other edition of SQL Server using the default installation settings then change all occurrences of .\SQLEXPRESS to (local) in ConnectionStrings.instance.config
- If you have a remote installation of SQL Server change all connection strings in ConnectionStrings.instance.config using the details provided by your database administrator (this is the hardest option to configure)

   Note: for appsettings.Production.json make sure any \ characters in the connection string are escaped as \\)

6) Copy appsettings.Production.json to C:\Program Files (x86)\PowerMapper Software\Phoenix Web App

7) Copy Server.instance.config and ConnectionStrings.instance.config to C:\Program Files (x86)\PowerMapper Software\Phoenix Service

8) Open the Windows Services administration tool and start the following three services:

   - Phoenix.EmailService (emails scan results)
   - Phoenix.HousekeepingService (deletes old scans)
   - Phoenix.ProcessService (runs queued scans)

9) Close all open browser windows to make sure session cookies have been cleared.

10) Open http://yoursever/SortSiteEnterprise/HealthCheck using a browser on a desktop PC. If the installation is complete all checks should show OK (see the section on Monitoring below). This might take 30-60 seconds to display the first time you view it.

   Important: you **MUST** be logged in as domain user before running setup (do not run it from a local machine account like Administrator). If necessary, run setup from a browser on your desktop machine replacing localhost with the name of the server.

11) Open http://yourserver/SortSiteEnterprise/Customer/Setup using Internet Explorer on the server. Enter the following then click Next:

   - Your organisation name
   - Your email address (will be used as the initial administrator account, and also as the sender address in emails sent by the system – can be changed later)
   - 'beta' as the serial number
   - The DNS name or IP address of an SMTP server name that will accept email from this server. This is used for new account invites, password resets, and emailing scan results. We recommend using localhost to utilize the local mail server setup earlier.
   - The SMTP server port (default for SMTP is 25)

   Note: You'll get a security exception if you try running /Customer/Setup

after the administrator account has been created. If you forget this password the you can use the Forgot Password link on the login page to email a password reset link. If you forget this password and email isn't setup correctly refer to the Troubleshooting section

12) Try using the Quick Scan box on the home page to test that everything is working. For the first scan it's best to use a small site (e.g. http://try.powermapper.com). Once the scan is done, the lower section of the first report might take 30-60 seconds to appear.

Note: Do not try to send New User invites when using the web application via http://localhost . If you do, then email invites will link back to http://localhost. You should only send invites when connected via a URL that everyone in the organization can access (either an IP address or DNS name visible to all workstations).

5.6 Deploying Scanner Upgrades

The scanner is largely independent of the rest of the application and is simple to upgrade:

1) Run CrawlerProcessFull.exe and install to default location.

5.7 Deploying Application Upgrades

This file describes how to migrate from a previous version of the application

Pre-Requisites

- A working installation of Enterprise Suite

Installation Files Required

- CrawlerProcessFull.exe
- EnterpriseServiceSetup.exe
- EnterpriseWebAppSetup.exe
- Rollout-012.sql (used to upgrade existing database schema)

Note: the database upgrade file has a different name each release based on the current schema version and the new schema version. There were no schema changes and no database upgrades in version 2021.1 or 2022.2

Upgrade Procedure

1) Go the Services administration tool and stop the following services:

    a) Phoenix.EmailService (emails scan results)
    b) Phoenix.HousekeepingService (deletes old scans)
    c) Phoenix.ProcessService (runs queued scans)

2) Run the Rollout-012.sql script on the Phoenix database in SQL Server Management Studio

3) Run EnterpriseWebAppSetup.exe as administrator and install to default location

4) Run CrawlerProcessFull.exe as administrator and install to default location

5) Run EnterpriseServiceSetup.exe as administrator and install to default location

6) Restart the services stopped above

7) Run the IISRESET /RESTART command at the command line

8) Open http://yoursever/SortSiteEnterprise/HealthCheck using a browser on a desktop PC. If the installation is complete all checks should show OK (see the section on Monitoring below). This might take 30-60 seconds to display the first time you view it.

9) Open http://yoursever/SortSiteEnterprise - you should see the home page and be logged in as an Administrator

Note:
The application uses anti-forgery session cookies to prevent HTTP request tampering. This can result in an error being displayed if

a) you upgrade the application
b) your browser has a window open showing one of the application's pages

This problem will disappear after closing all open browser windows (and will clear itself within 24 hours when the cookie expires).

5.8 Migrating to a Remote SQL Server

When the database is hosted on a different machine than the web application, some additional configuration is needed. In summary, the additional steps are:

1) Backup the SQLEXPRESS database from the SortSite web server and restore on the dedicated SQL Server
2) Run the AddServiceAccount.sql script on the dedicated SQL Server
3) Change the database connection strings on the SortSite web server
4) Change the service logins for the 3 Phoenix services in the Services console on the SortSite web server

In addition to these steps, you need network connectivity between the web server and the database server on the TCP port used by SQL Server (the default port is 1433). This may require some router/firewall configuration if firewalls protect the web server or database server.
The detailed steps are:

1) Backup the Phoenix SQLEXPRESS database for the SortSite web server and restore on the remote SQL Server using SQL Server Management Studio

2) Run the AddServiceAccount.sql script on the server the database was restored to. This script creates a service account for the computer running the Enterprise Suite web server, allowing the web server to access the database. Note that the script needs modified with your domain name and the computer name of the SortSite web server (see the instructions in AddServiceAccount.sql)

3) Change all the connection strings in:

- c:\Program Files (x86)\PowerMapper Software\Phoenix Web App\ appsettings.Production.json
- c:\Program Files (x86)\PowerMapper Software\Phoenix Service\ ConnectionStrings.instance.config

The parts of the connection strings reading Data Source=.\SQLEXPRESS needed changed to Data Source= YOUR_SQL_SERVER, where YOUR_SQL_SERVER is the name of the database server on the network.

Make sure you keep a copy of these changes, so you can reapply them after upgrades.

4) Change the service logins from Local Service to Local System in the Services console on the SortSite web server for the following services.

- Phoenix.EmailService
- Phoenix.HouseKeepingService
- Phoenix.ProcessService

This is required because the Local Service account doesn't have network access rights, which are required to connect to the remote SQL Server.

6 Configuration

6.1 Web Application

The web application database connection strings are in c:\Program Files (x86)\PowerMapper Software\Phoenix Web App\ appsettings.Production.json

Configuration File Settings	Value
ConnectionStrings / PhoenixWebApp	Connection string to database (only the part following "provider connection string" should be changed)

The web application configuration file is c:\Program Files (x86)\PowerMapper Software\Phoenix Web App\Web.config

Configuration File Settings	Value
Healthcheck_CheckList	Controls list of healthchecks carried out
Healthcheck_CheckServiceList	List of Windows Services which must be running

Healthcheck_ProcessQueue_TimeoutPerPageSecs	Healthcheck complains if pages take longer than this to scan (very large files like videos can take a long time to download and scan)
Healthcheck_ProcessQueue_MissedScheduleSecs	Healthcheck complains if a scan is waiting longer than this to start
Healthcheck_ProcessQueue_PendingCount	Healthcheck complains if more than this number of scans are queued
Healthcheck_EmailQueue_TimeoutSecs	Healthcheck complains if emails take longer than this to send
Healthcheck_EmailQueue_MissedScheduleSecs	Healthcheck complains if an email waits longer than this before being sent
Healthcheck_Server_Config	Path to PhoenixService server.instance.config
Healthcheck_Service Config	Path to PhoenixService.exe.config

6.2 Windows Service

The service database connection strings are in c:\Program Files (x86)\PowerMapper Software\Phoenix Service\ConnectionStrings.instance.config

Configuration File XML Path	Value
configuration/connectionStrings/add[WebAppEntities] configuration/connectionStrings/add[ServiceEntities]	
connectionString attribute	Connection string to database (only the part following "provider connection string" should be changed)

The service instance configuration file is c:\Program Files (x86)\PowerMapper Software\Phoenix Service\Server.instance.config

XML Path	Value
applicationSettings/ Phoenix.Service.Properties.Settings	
ServerName	Should always be app11
ServerUserId	Should always be 1
TempDirectory	On a storage volume with enough space to store an entire scan (typically same volume as reports)

The service configuration file is c:\Program Files (x86)\PowerMapper Software\Phoenix Service\PhoenixService.exe.config

XML Path	Value
system.diagnostics/trace/listeners/add[ServiceLog]	
initializeData	Path to text log for service

6.3 DNS

Once the server is up and running you should assign an internal DNS name. Without a DNS name your users will need to connect to it with an IP address

7 Troubleshooting

Problem	Cause	Resolution
Unrecognized attribute targetFramework when you try to display the web application	The .NET 4.0 web application is running in a .NET 2.0 application pool	Ensure the IIS application pool used by the web application uses .NET Framework 4.0
Running PhoenixWepApp.exe says it requires IIS 5.0 or later	IIS is not installed by default on Windows Server 2008	Follow the IIS installation instructions above
A 403.14 error appears when you try to display the web application	.NET Framework 4.0 is not properly registered with IIS	Use the .NET 4.0 version of aspnet_regiis –i
A timeout message appears connecting to the database	Either cannot connect to SQL Server (firewall or network issue) or the connection string doesn't match the SQL Server instance name (the default connection string matches the default instance name of SQL Server Express)	Check the instance name in web.config and if it's correct check that the SQL Browser service is running in the Services MMC console
Cannot start services	Check event log – most likely cause is wrong connection string or failed SQL Server login	Check connection strings in PhoenixService.exe.config then check SQL Server logs
Web app says it cannot login to database	Connection strings don't match database login credentials	Check connection strings in Web.config and if they're correct check SQL Server logs
The (>>) expansion buttons don't work in reports viewed using Internet Explorer on the server via Remote Desktop	By default Internet Explorer won't run JavaScript when installed on Windows Server	Expected behavior: view the report from a desktop PC
User or administrator has forgotten their password		Use the Forgotten Password link on the login page
Administrator has forgotten their password **and** email is not setup correctly	Password reset emails cannot be sent if email is not setup correctly	Use the Forgotten Password link on the login page Connect to database via SQL Management Studio Run this SQL "select EmailAddress,ResetKey from Security.AuthorisedUser where ResetKey is not null" Open the following URL in a browser adding the ResetKey to the end: http://localhost/SortSiteEnterprise/Account/Reset Password?key=
Other problems		Use HealthCheck to diagnose

8 Monitoring

The web application provides an unauthenticated /HealthCheck page which checks system status. This can be opening in a browser on the server hosting OnDemand using the following address:

http://localhost/SortSiteEnterprise/HealthCheck

This can be polled by monitoring tools. When the page detects an error then **HealthCheck: Fail** is added to the list of HTTP headers returned by the page. The HealthCheck page appears like this when the application is running normally:

	Check	Status
↑	CheckCrawlerExes	OK
↑	CheckServerExeRunning	OK: PhoenixService;
↑	CheckRunningServices	OK: ProcessService.Service;EmailService.Service;HousekeepingService.Service
↑	CheckDBConnectivity	OK
↑	CheckDBProcessQueue	OK
↑	CheckDBEmailQueue	OK
↑	CheckPermissions	OK
↑	CheckFailover	OK
↑	CheckDiskSpace	OK

The HealthCheck page appears like this when a problem is detected:

	Check	Status
↑	CheckCrawlerExes	OK
↑	CheckServerExeRunning	OK: PhoenixService;
↓	CheckRunningServices	Fail: System.Exception: Stopped services: ProcessService.Service at PhoenixWebApp.Controllers.HealthcheckController.CheckRunningServices() in C:\Projects\Electrum\Mapper\Web\Phoenix\PhoenixWebApp\Controllers\HealthcheckController.cs 216 at PhoenixWebApp.Controllers.HealthcheckController.AddCheck(String checkName, String displayName, HealthCheckDelegate check) in C:\Projects\Electrum\Mapper\Web\Phoenix\PhoenixWebApp\Controllers\HealthcheckController.cs 92
↑	CheckDBConnectivity	OK
↑	CheckDBProcessQueue	OK
↑	CheckDBEmailQueue	OK
↑	CheckPermissions	OK
↑	CheckDiskSpace	OK

In this example one of the Windows services the application relies on has been stopped.

9 Security

9.1 Database Connections

By default, the Web App and Service components connect to local instances of SQL Server using built-in Windows service accounts (Local Service for the PhoenixService and Network Service for the web app). For connection to a remote SQL Server dedicated domain service accounts (or SQL server logins) need created with the credentials specified in the connection string in Web.config and PhoenixService.exe.config (see Configuration above).

9.2 Securing Data

Data	Default Security	Enhanced Security
User Email Addresses	Stored as plain text in database	Use SQL Server Transparent Data Encryption (TDE) to encrypt entire database (only available with SQL Server Enterprise)
User Passwords	Stored as one-way encrypted SHA1 hash (with salt) in database.	Use TDE
Addresses of scanned sites	Stored as plain text in database	Use TDE
Scan Reports	Stored in file system protected by ACLs	Restrict ACLs on reports folder Enable NTFS encrypting file system (EFS) on reports folder
Optional form data used during scans. Users can use this feature to enter usernames and passwords for login forms (so data is encrypted).	Stored AES encrypted in database. AES key is randomly generated at install time and stored in registry. Key should be backed up with a registry backup utility.	Use TDE

Note: enabling TDE encryption on SQL Server, or EFS encryption on the file system, renders the data permanently inaccessible if the encryption keys are lost. Only use these options if you have tried and tested procedures in place to prevent loss and allow recovery of encryption keys.

10 Backup and Restore

10.1 Data to backup

Data	Location	Backup and Restore
Phoenix Database	SQL Server	Use standard SQL Server backup procedures and tools
Scans and sitemaps folders	C:\SS.NET\Maps C:\SS.NET\Reports	Use standard file backup procedures and tools
Phoenix encryption key	Registry: HKLM\Software\Wow6432Node\PowerMapper Software\Shared:EK	Use standard Windows registry backup procedures and tools.

Note: in the event the encryption key is lost/deleted, entered form data is unrecoverable, but can be re-typed. No other data is encrypted with the key, so loss is likely to be inconvenient rather than disastrous. Scans without any form data entered are unaffected by loss of the key.

10.2 Fresh Install

To do a fresh install without data on a clean copy of Windows follow these steps:

1) Install platform and application using the instructions in the Deployment section of this document

10.3 Bare Metal Restore

For a bare metal restore follow these steps:

1) Install platform and application using the instructions in the Deployment section of this document
2) Restore the Phoenix database
3) Restore C:\SS.NET\Maps and C:\SS.NET\Reports
4) Restore the encryption key registry entry

11 Known Problems and Limitations

. Using form playback settings on sites with an anti-forgery cookie.

Problem: You may see a 500 Server Error scanning ASP.NET MVC sites using Form and Login settings.

Cause: Some websites set a cookie to mitigate against replay attacks on login forms. The site being scanned tries to set a cookie, but the scanner process doesn't run with enough permissions to allow the cookie to be set.

Workaround: In Windows Services management console change the Log On as settings for the Phoenix.ProcessServices.Service from Local Service to .\Administrator. This grants the scanner process enough rights to allow cookies to be set.