nFront Web Password Change

Version 3.0.0

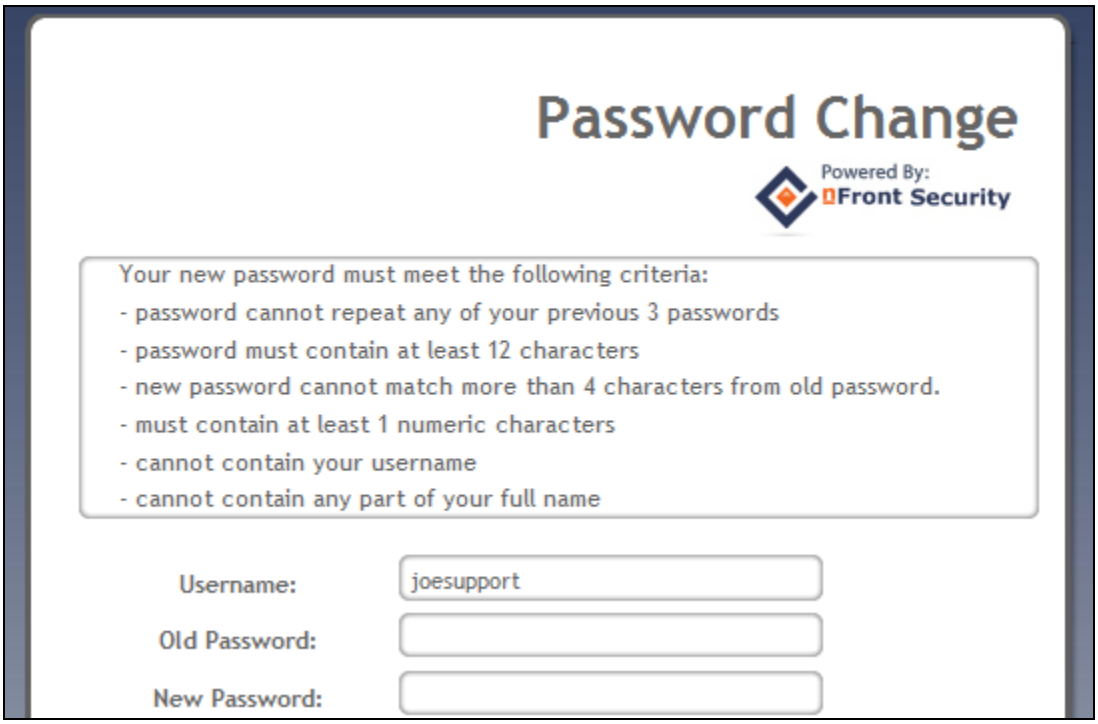
Documentation

Contents

NOTE: Please report any problems with this document to feedback@nFrontSecurity.com. Your feedback is important and we sincerely appreciate your help.

1.0 Overview

The nFront Web Password Change is a password change web application for Active Directory users which is “nFront Password Filter aware.” It will dynamically display the list of password requirements for the user and a very detailed failure message of the password is not accepted.



1.1 Requirements:

- Windows 2000, 2003 (x86 or x64), 2008 (x86 or x64), 2008 R2 or Windows Server 2012. The server may be a member server or a domain controller.
- Internet Information Server
- .NET Framework 3.5 or later installed
- nFront Password Filter installed on all domain controllers

1.2 What’s New

What is new in Version 3.0?

- *CSS modifications to look better in Internet Explorer 9.*
- *x86 and x64 versions for Windows 2003, Windows 2008*
- *Additional error cases for accounts that are disabled or password is less than the minimum age.*

What is new in Version 2.0?

- *It can block a password change to a similar password. This rule was added to nFront Password Filter 4.16 but requires support from the client and web interface.*

- *A registry value for "successURL" was added to redirect a successful password change to a different web page.*
- *You can turn on debugging to see error codes for failed password changes. This is handy when troubleshooting network or firewall configuration issues.*
- *The "Test Password" button is now optional and requires a registry modification to display the button.*
- *Requirements window automatically sizes to list all rules (with no scroll bars).*

What is new in Version 1.2?

- *A button labeled "Test Password" was added to allow users to test a potential password before changing to it.*

2.0 Installation

2.1 Installation Requirements.

There are 2 MSI packages (one for x86 machines and one for x64 machines). The package may be installed on a domain controller or a member server. The server must have Internet Information Server and ASP.NET 3.5 or later.

You will need to be sure ASP .NET is enabled on the server. During the installation you can select the website and virtual directory target.

IMPORTANT: If you have Windows 2008 or Windows Server 2012 you must install IIS Metabase Compatibility (Figure 2.1.3). If you do not do this the installer will not complete.

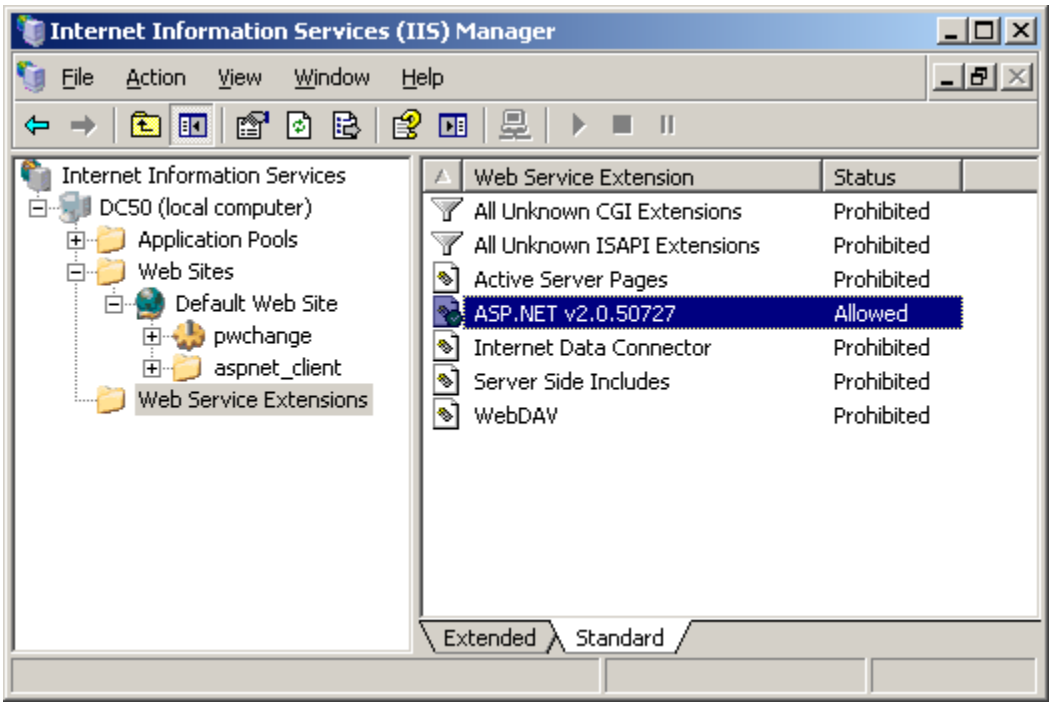


Figure 2.1.1 – ASP.NET allowed on Windows 2003 Server

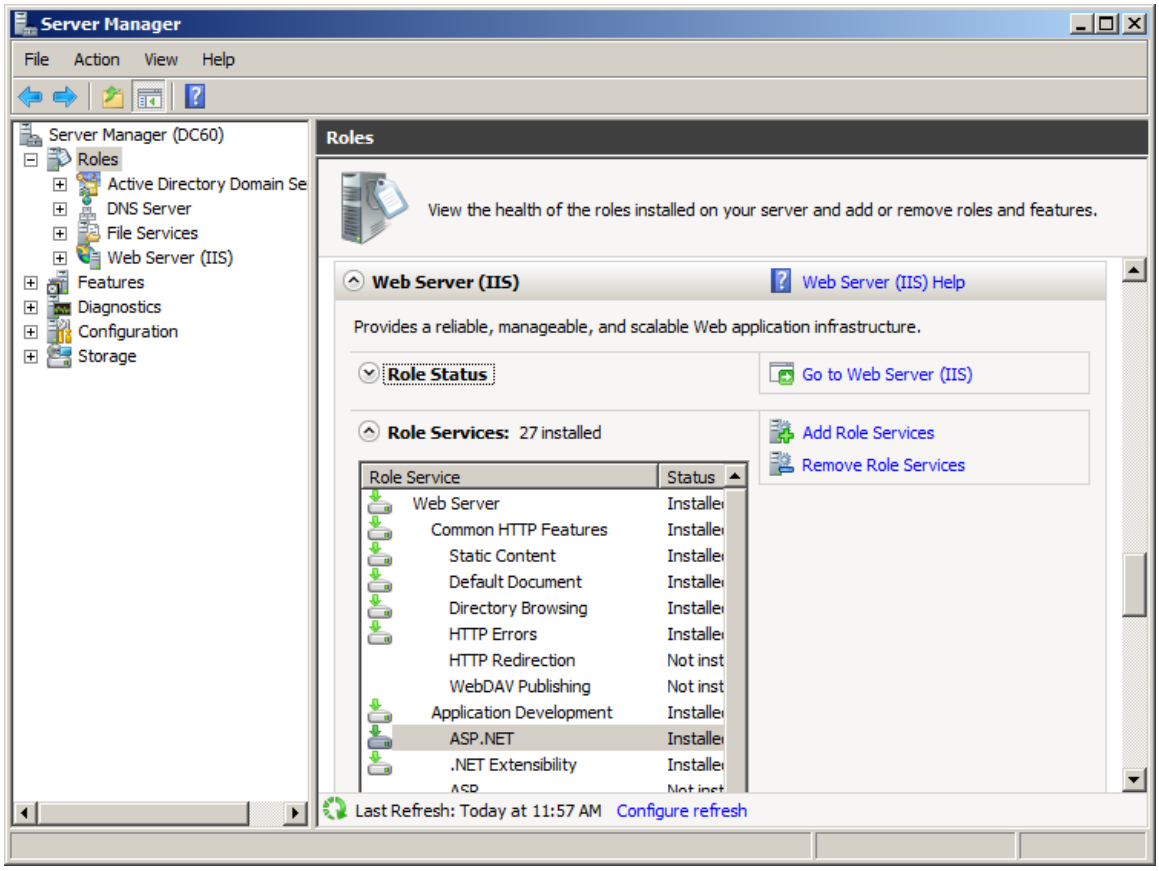


Figure 2.1.2 – ASP.NET allowed on Windows 2008 Server

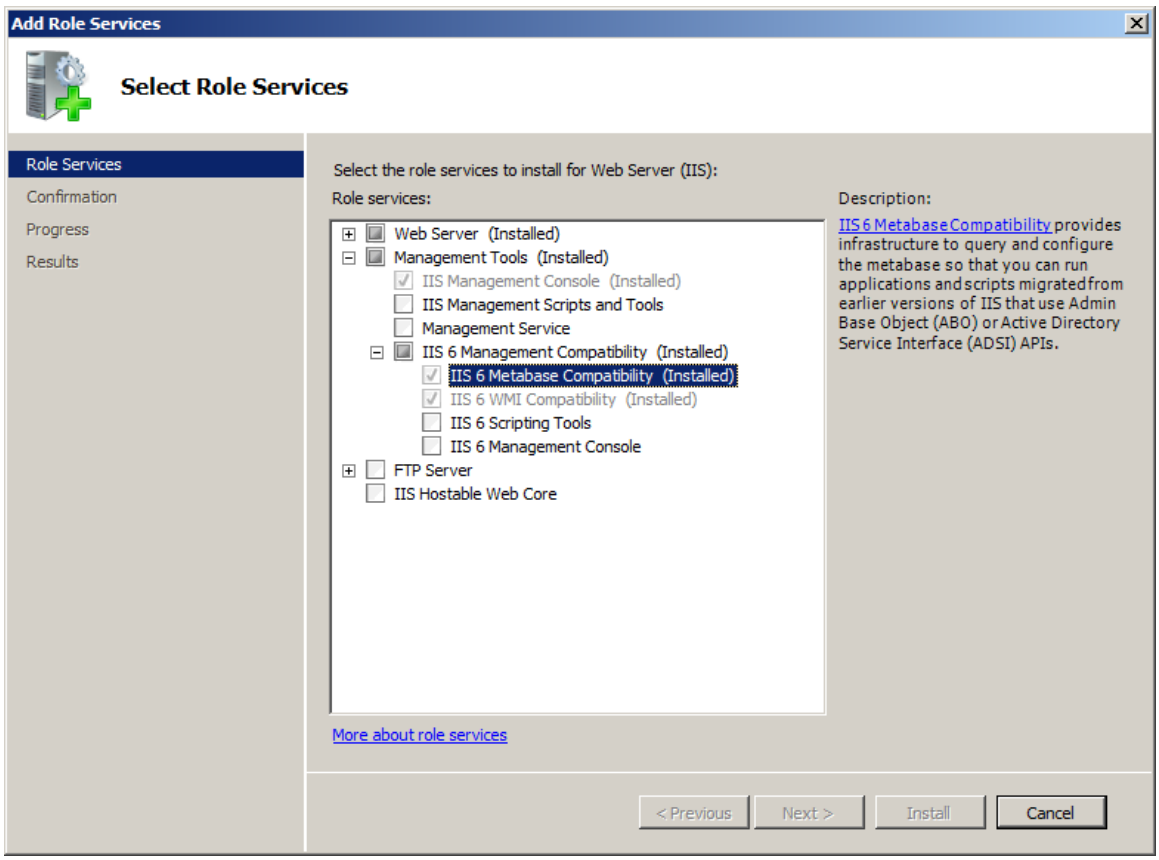


Figure 2.1.3 – Adding IIS 6 Metabase Compatibility on Windows 2008

2.2 Installation Screenshots

Just double-click the nFront Web Password Change.MSI (or the x64 version) to launch the setup program.

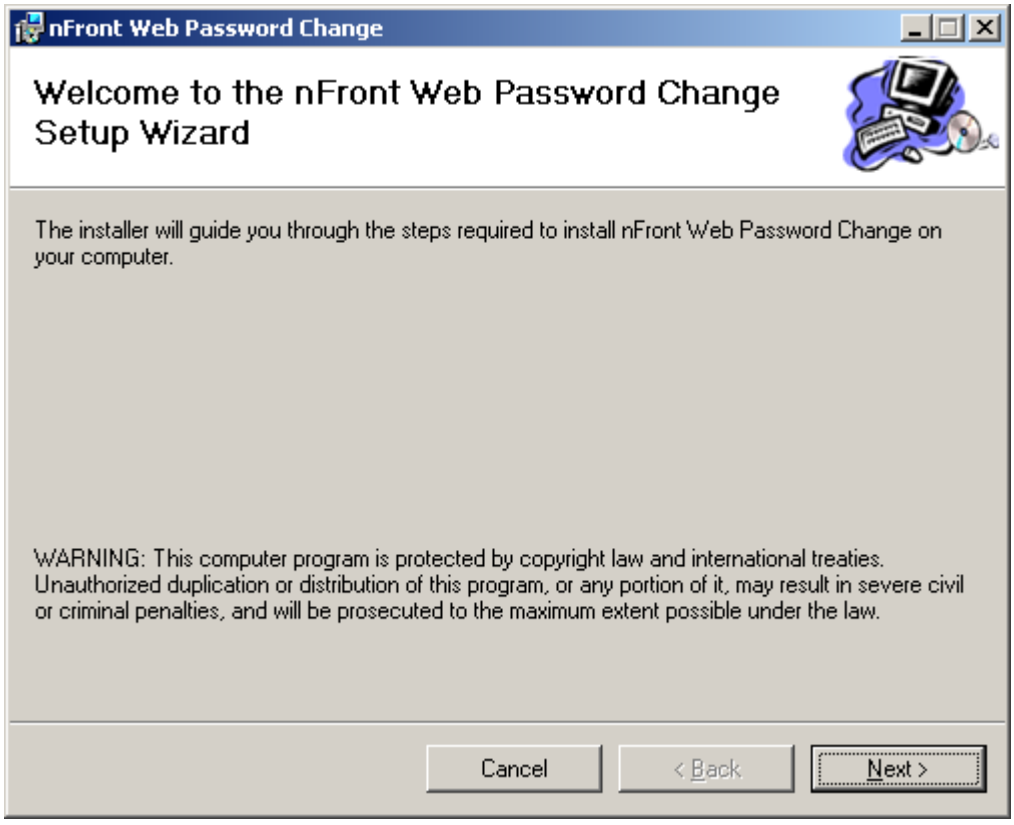


Figure 2.2.1 – Installation wizard – step 1

You can select the website and virtual directory on this screen. The virtual directory you select will determine the URL to access the application (i.e. http://<server>/<virutal directory>). If you are installing on Windows 2008 then you must select Classic .NET AppPool in the Application Pool drown down listbox. If you are installing on Windows 2003 you can leave the default selection of DefaultAppPool.

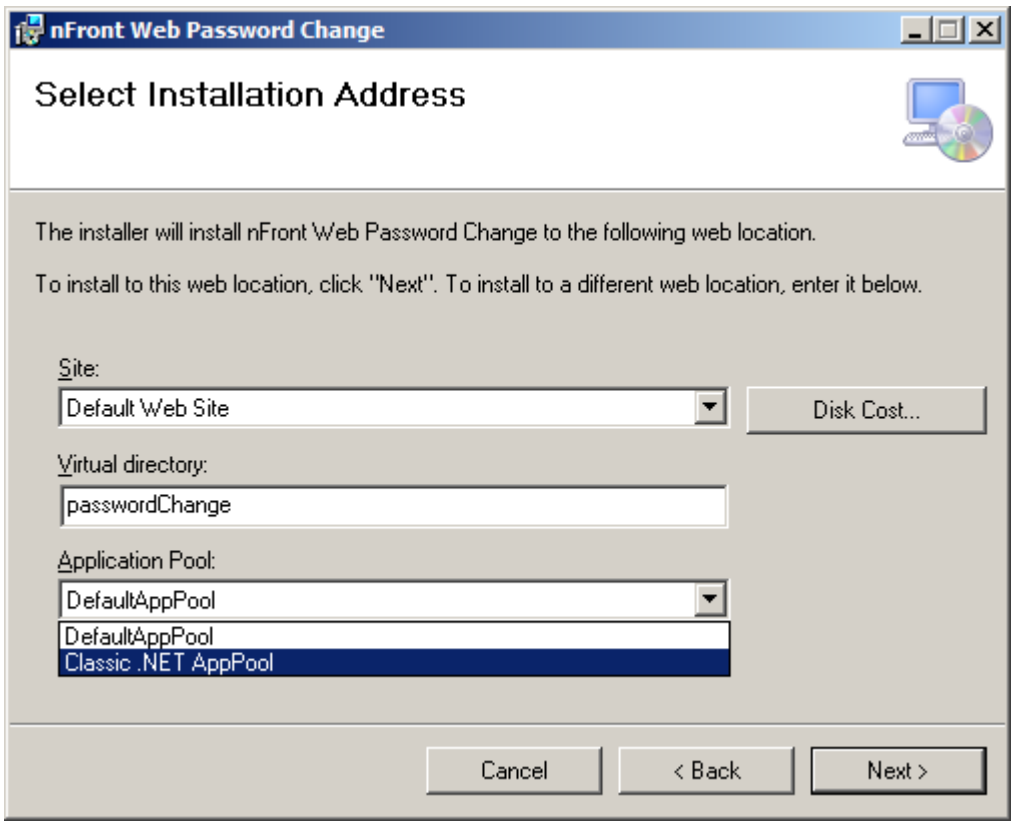


Figure 2.2.2 – Installation wizard – step 2

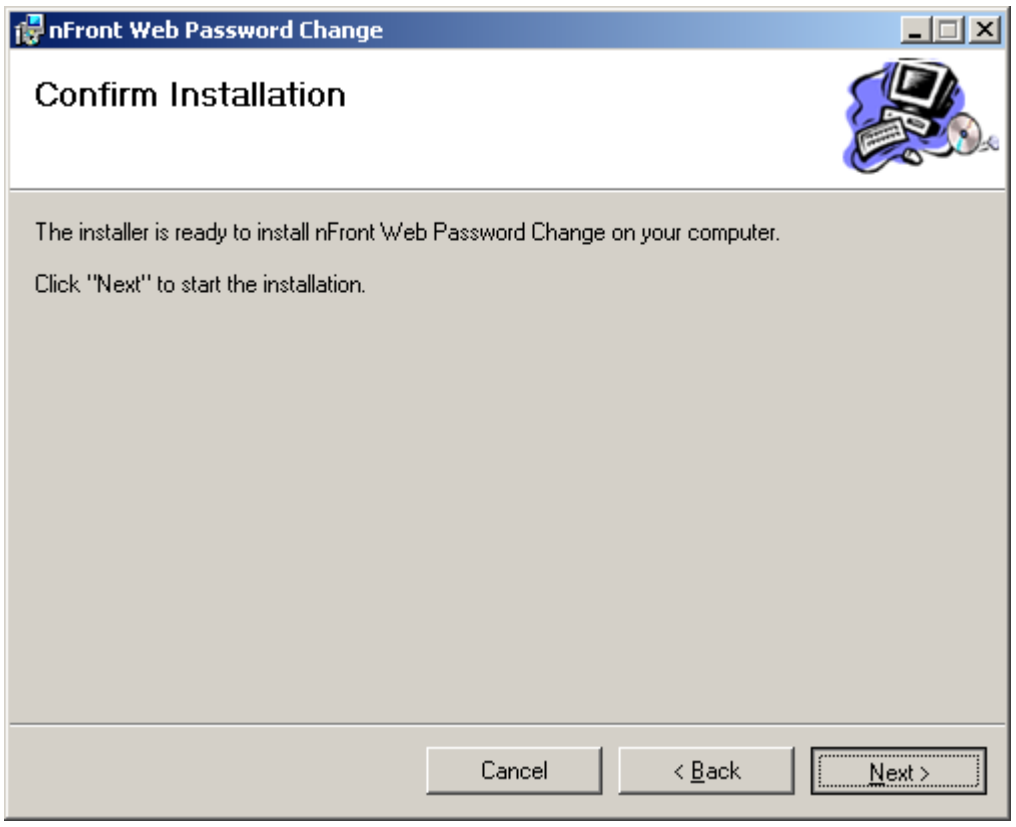


Figure 2.2.3 – Installation wizard – step 3

You will be prompted during installation for a Registration Code. However, a registration code is not necessary to evaluate the software and you may register the software easily later using an application in the Start Menu. If you are evaluating the software just click OK to move forward.

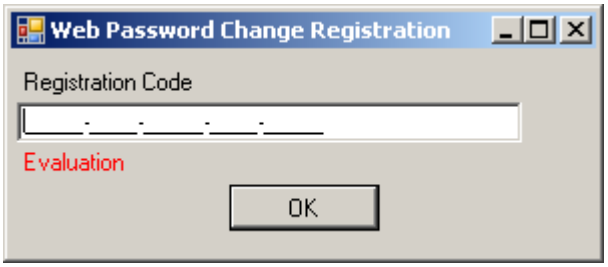


Figure 2.2.4 – Optional registration

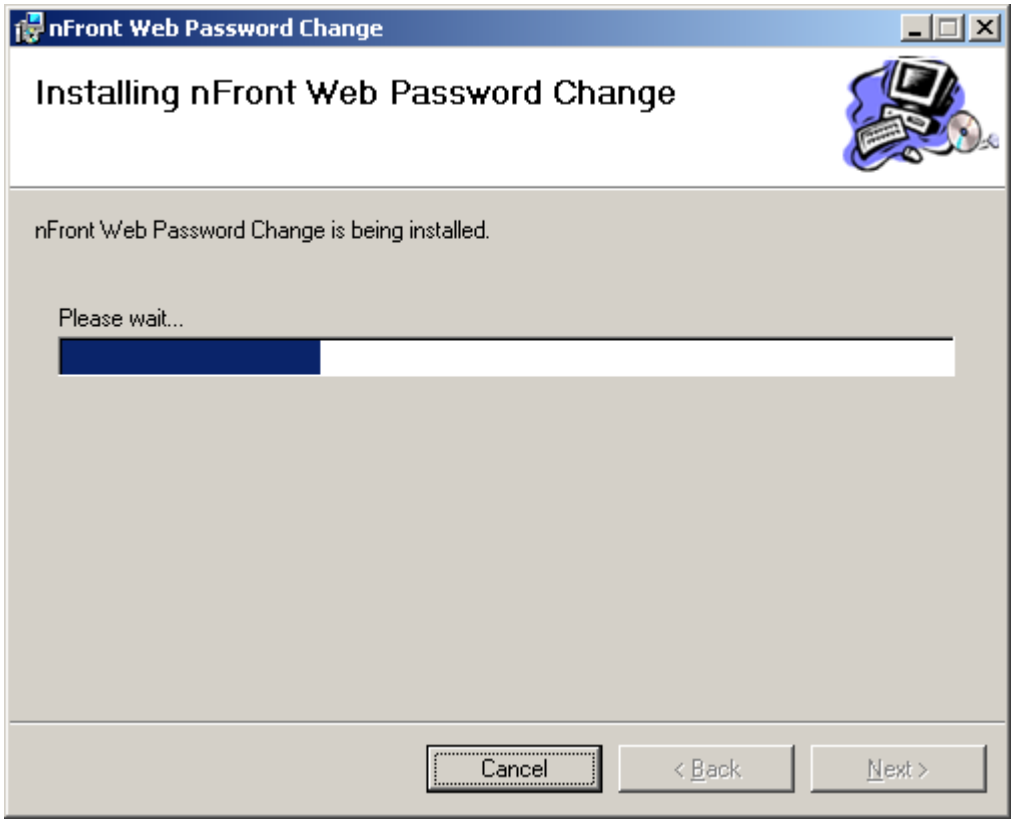


Figure 2.2.5 – Installation of files

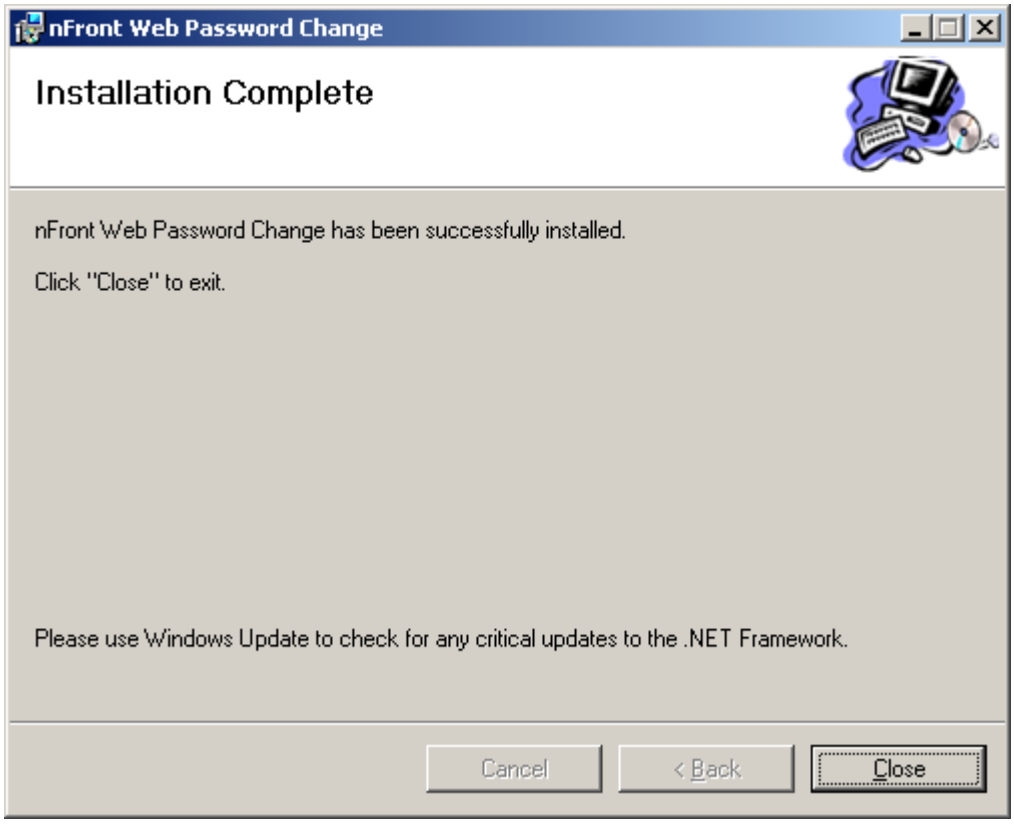


Figure 2.2.6 – Installation completion

After the installation completes you may wish to launch the IIS Manager to confirm the site and virtual directory used during the installation.

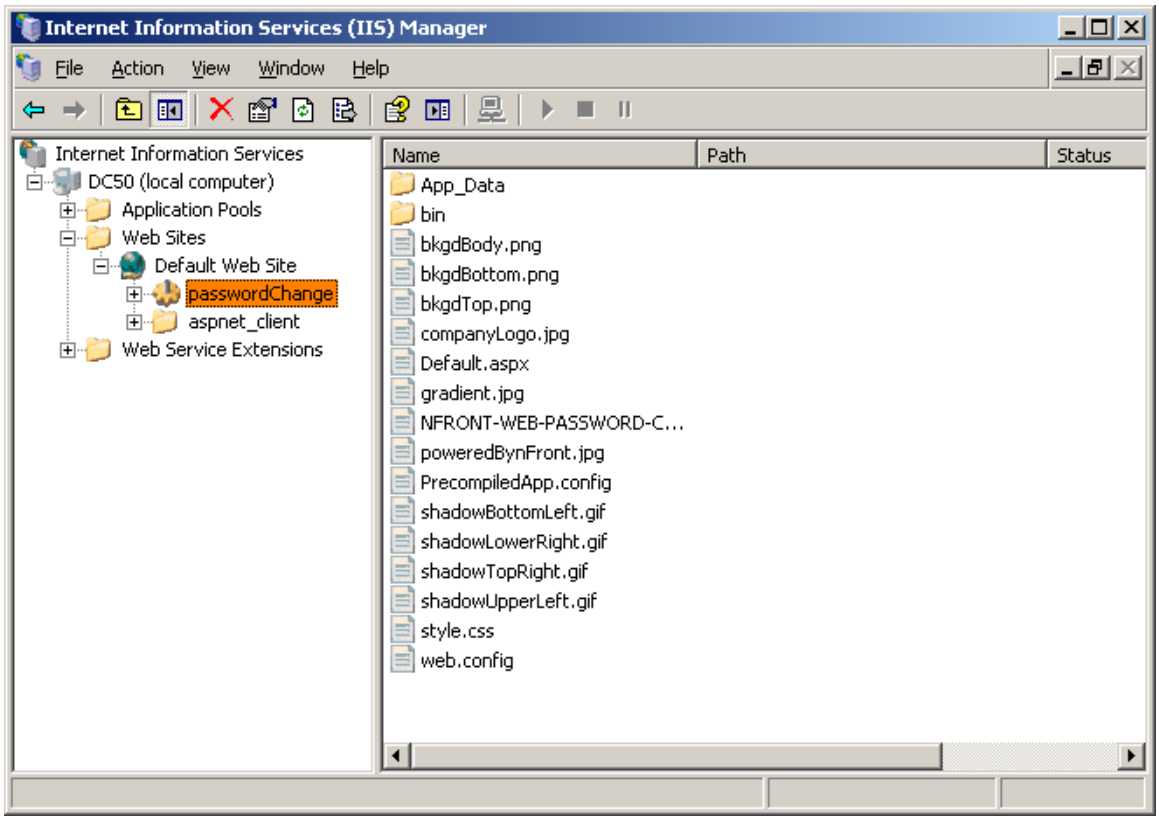


Figure 2.2.7 – IIS Manager with virtual directory on Windows 2003

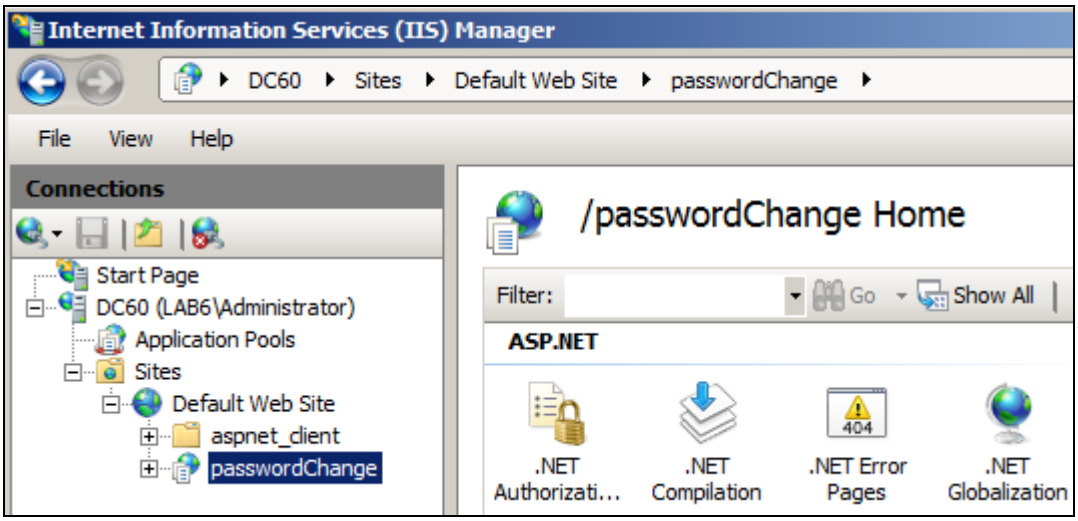


Figure 2.2.8 – IIS Manager with virtual directory on Windows 2003

2.3 Check the Installation

You can simply open a web browser and go to http://<machine-name>/<virtual directory> or http://localhost/<virtual directory>. If you chose a different site or port number you will need to use that in the URL. You should see a screen like the one below in Figure 2.3.1.

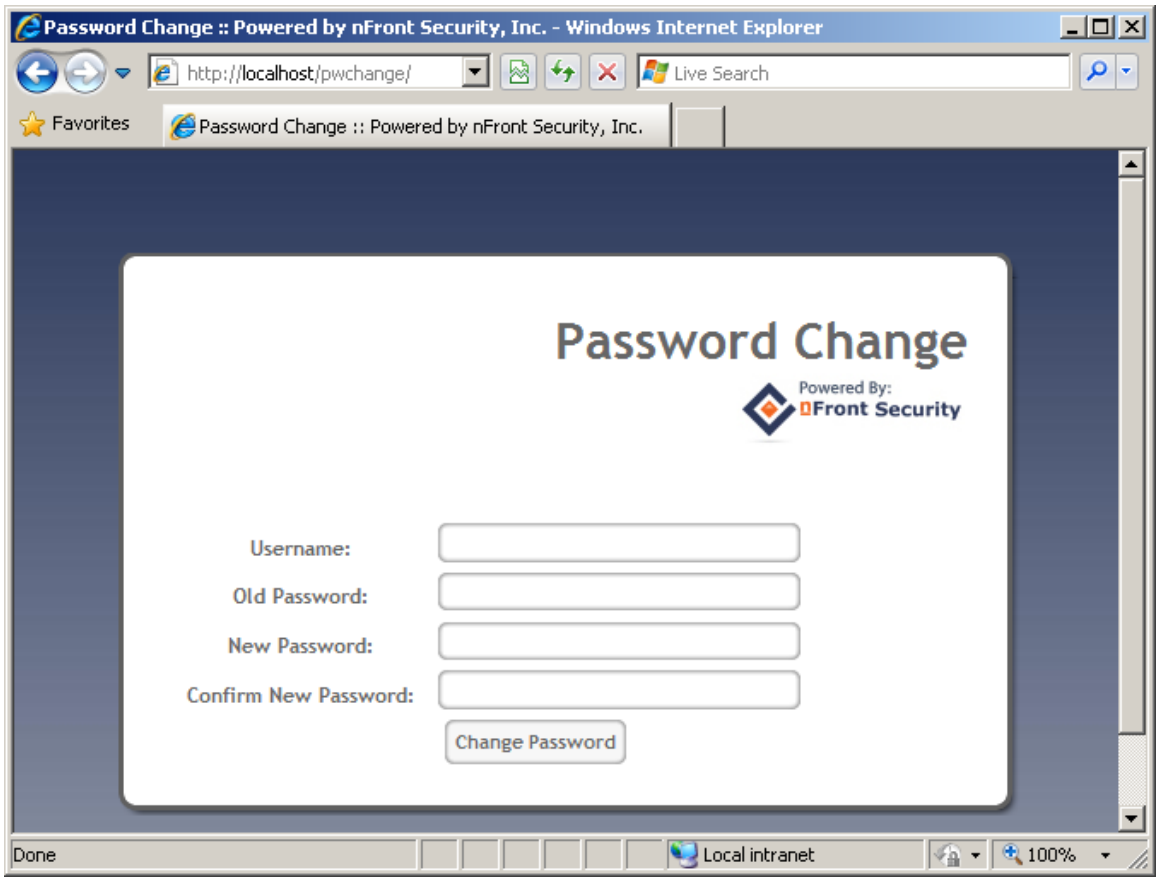


Figure 2.3.1: nFront Web Password Change screen in Internet Explorer

If you are prompted for authentication when using http://localhost/<virtual directory> then you may need to check the permissions on the virtual directory to ensure the directory is configured for Integrated Windows Authentication and anonymous access is disabled. Use Internet Information Services (IIS) Manager to navigate to the website + virtual directory + right-click and select properties + Directory Security tab (Figure 2.3.2). In the Authentication and Access Control section click the Edit button to edit the Authentication Methods. Be sure the system is configured for Integrated Windows Authentication and there is no check for Enable Anonymous Access (Figure 2.3.3).

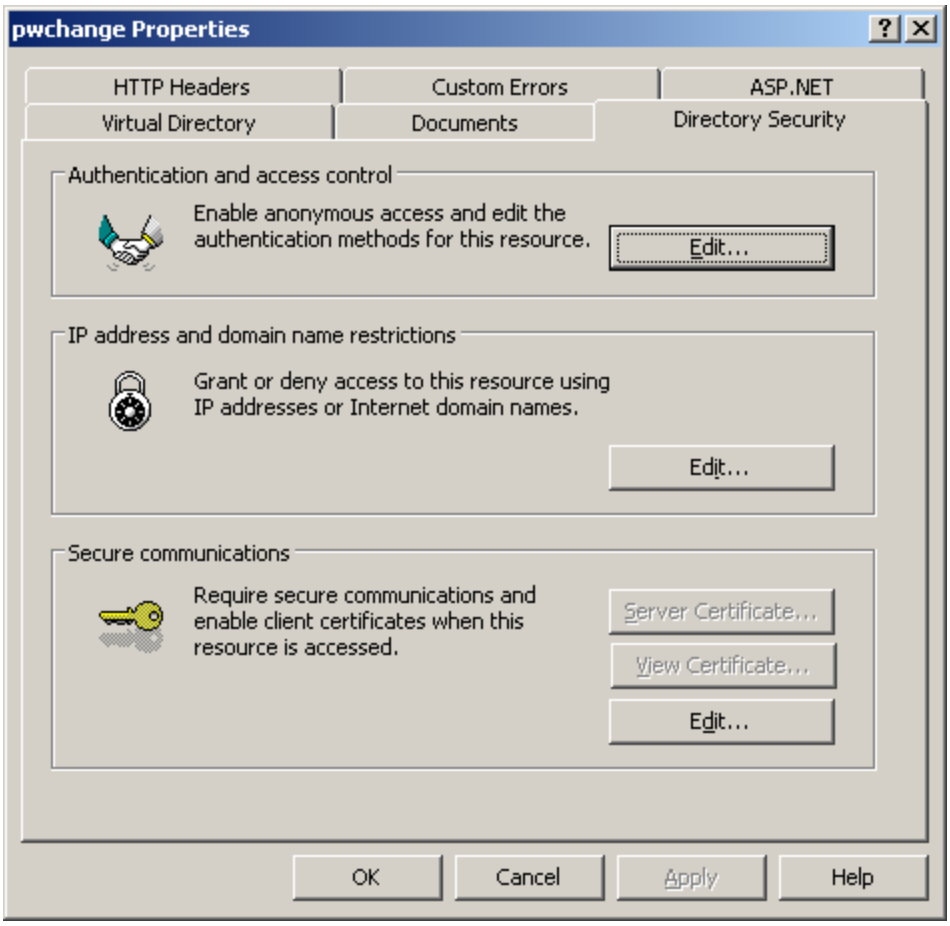


Figure 2.3.2: Properties of virtual directory for application

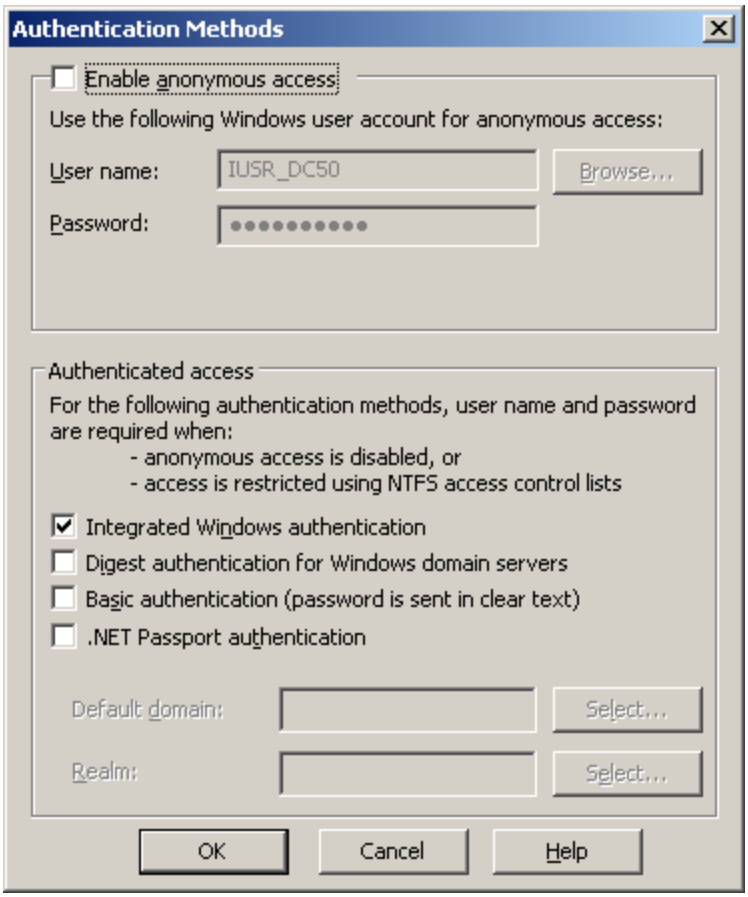


Figure 2.3.3: Authentication Methods for web application virtual directory

2.4 Fixing the problem with the Authentication prompt

If you modify your DNS to point to the server running nFront Web Password Change you will likely notice an authentication prompt when you attempt to connect to a location like "intranet.xyz.local/pwchange" (Figure 2.4.1).

Any browser other than Internet Explorer will always prompt for authentication when you make your initial connection to the web application.

Internet Explorer will perform integrated authentication (and not prompt the user) but only under certain conditions. According to KB article 258063 (http://support.microsoft.com/kb/258063), IE assumes the address is an internet address if the address contains periods. The solution is to add the website address to the Local Intranet. You can do this manually on each browser or via Group Policy. The Microsoft Knowledge Base says you should consult the IE Resource Kit for information on using Group Policy to distribute modifications to the Local Intranet settings of all browsers. There are many good Internet articles that cover this topic. Here is a good example: http://www.makeuseof.com/tag/configure-trusted-sites-internet-explorer-group-policy/.

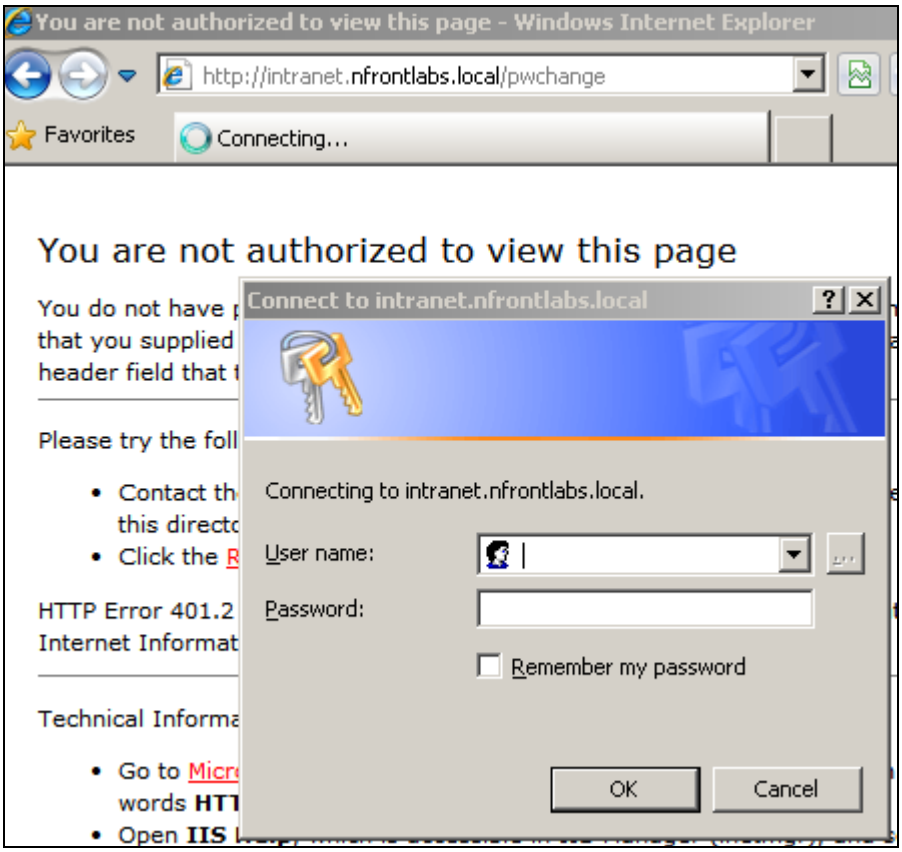


Figure 2.4.1: IE does not perform integrated windows authentication when URL contains periods.

In the next section you can find instructions to modify Internet Explorer to perform integrated windows authentication when contacting your internal website.

2.4.1 Manually modifying Local Intranet settings in Internet Explorer

In Internet Explorer go to Tools + Internet Options + Security Tab (Figure 2.4.1A)

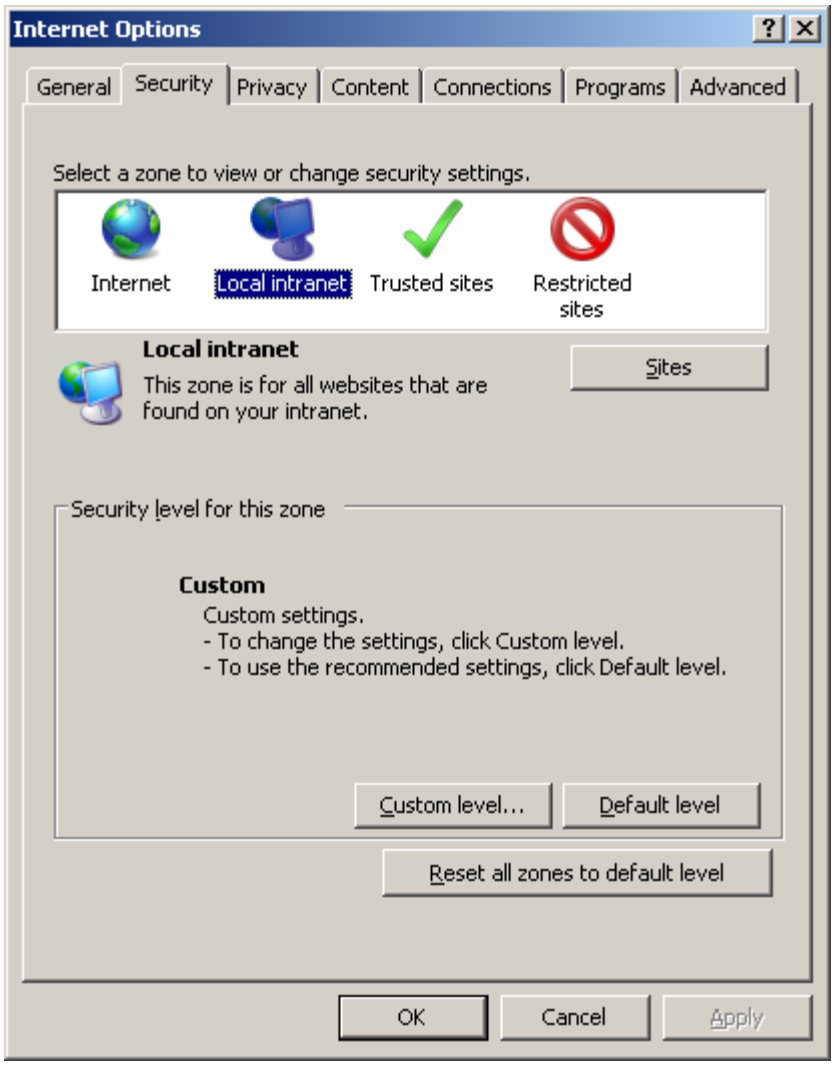


Figure 2.4.1A: IE Security Zones

In the Zones area select the Local intranet zone and click on the Sites button so go to the Local intranet settings (Figure 2.4.1B).

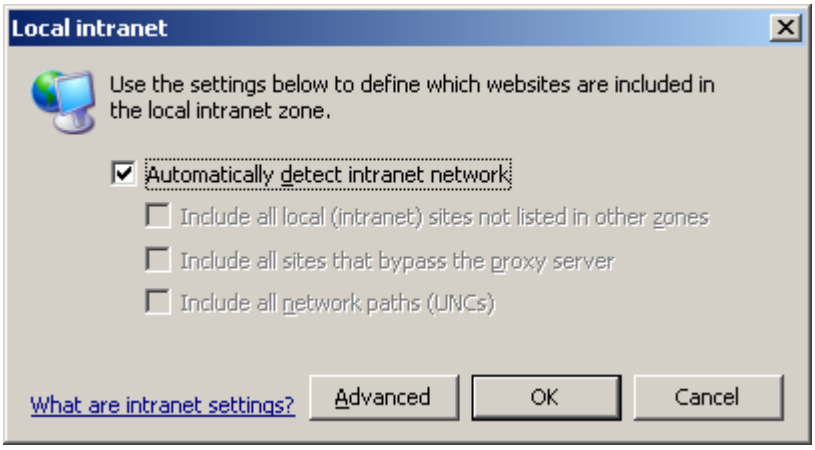


Figure 2.4.1B: IE Local intranet zone settings

Click on the Advanced button to add your website to the zone (Figure 2.4.1C). In the example below the URL is not https. On your network you should have your site secured with SSL to prevent clear text communication between the IE client and nFront Web Password Change on the server.

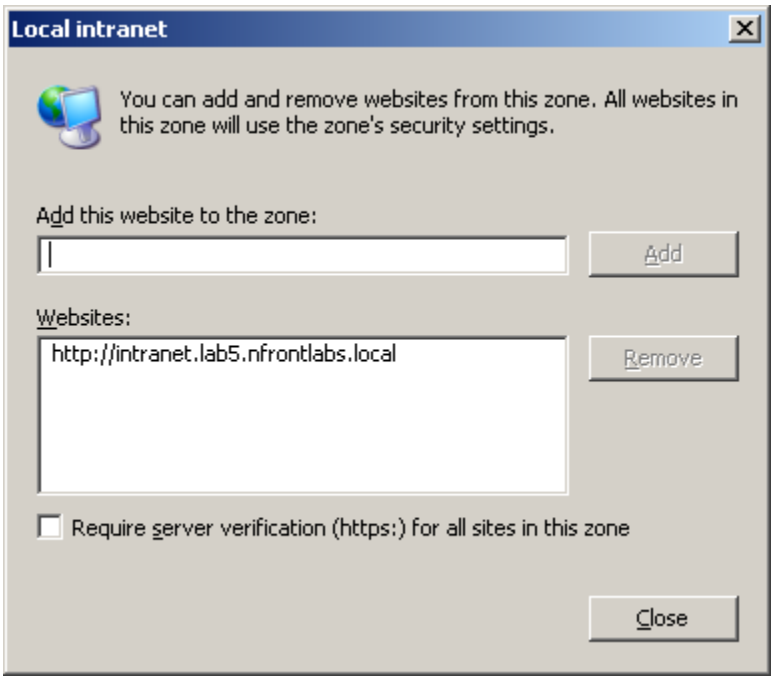
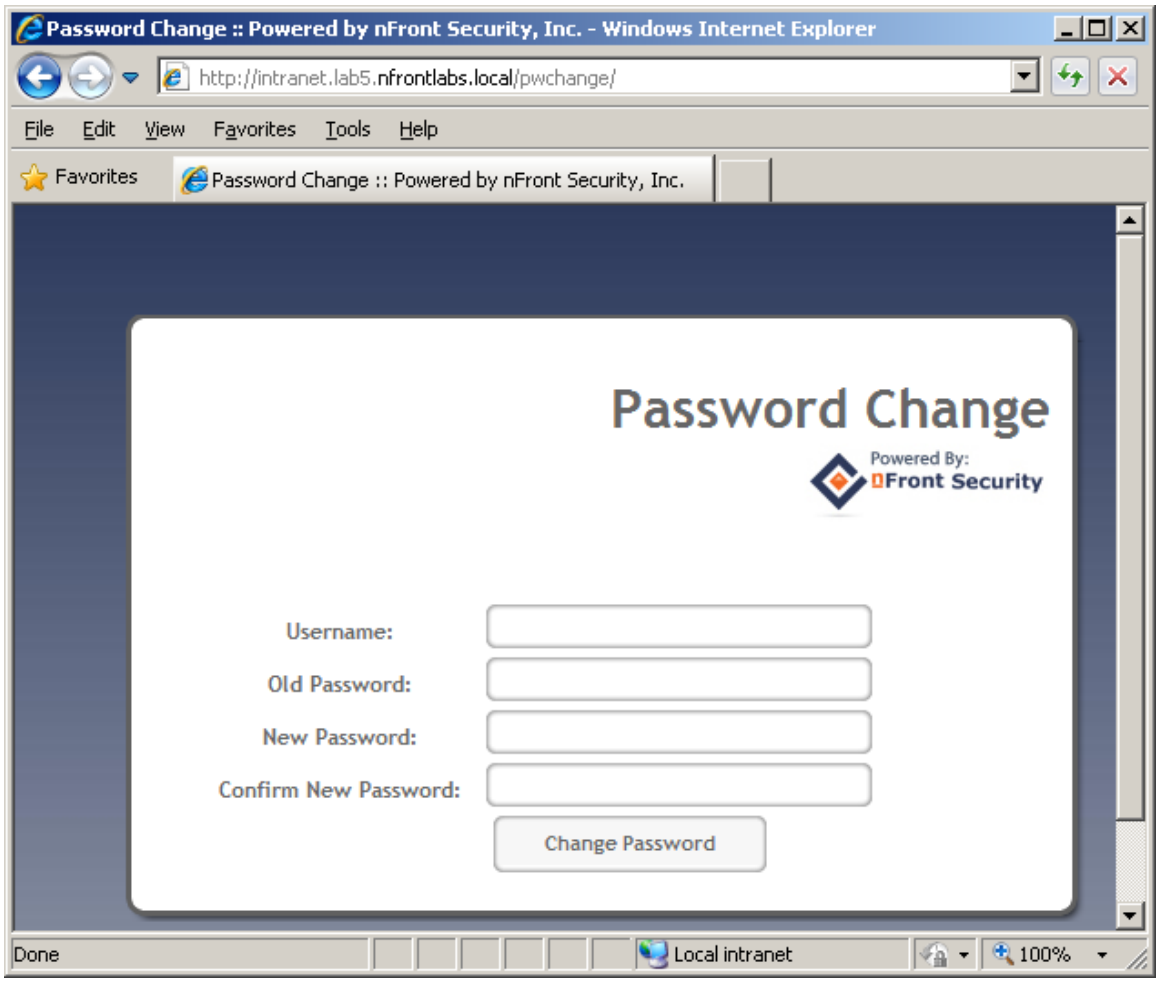


Figure 2.4.1C: Adding a new website to the Local intranet zone

After the change you should be able to navigate to the website with no prompts for authentication if using Internet Explorer.



2.5 Securing the site with SSL

You should never run the website internally or externally without using SSL to secure the site. Without SSL the communication from the Internet Explorer (or other) clients to the server will not be encrypted. Thus, it would be trivial to obtain clear text passwords.

If nFront Web Password Change is running on a member server it will need to communicate with a domain controller to get a list of password requirements and to test the password against the policies configured in nFront Password Filter. This communication is done using encrypted RPC from a DLL on the web server (altusgina.dll) and the nFront Password Policy Service on a domain controller. The service listens on port 1333. If you are running Windows 2008 domain controllers you must enable this port on the firewall. See the online nFront Knowledge Base for information on doing this.

You should apply an SSL certificate to the website on which the application runs. Instructions for obtaining and applying an SSL certificate are not covered here. However, any reputable vendor of SSL certificates will provide you with detailed instructions on the installation and configuration of SSL on your IIS server. Generally speaking it is a very simple process. nFront Web Password Change has been tested and verified to work fine with SSL.

2.6 Customization

You can customize companyLogo.jpg to your liking. The new logo file should have the same name and a dimension of 200 by 65 pixels.

nFront Web Password Change stores its registry settings in the following location:
HKLM\Software\nFront Security\Web Password Change

HKLM\Software\nFront Security\Web Password Change\useOriginalFailureText , REG_DWORD	Set to 1 if using NPF 4.13 or earlier.
HKLM\Software\nFront Security\Web Password Change\displayTestButton, REG_DWORD	Set to 1 to show the test button. This exposes a button for the user to click to test their password against nFront rules. Please note the password fields will be erased after clicking the button so after testing the user will need to re-type their old and new password. This is a security issue and maintaining data in the fields after the form submission would present the opportunity for a security compromise.
HKLM\Software\nFront Security\Web Password Change\debug, REG_DWORD	Set to 1 to turn on debugging. This is only used to debug firewall issues. When a non-standard error is returned it will be displayed in the web browser. There is no debug log file or a running log to reference.
HKLM\Software\nFront Security\Web Password Change\successURL, REG_SZ	If you use a value like “www.cnn.com” the application will treat it like a relative URL and append it to the current URL. You must use “http://” to have the application treat it as an absolute URL.
HKLM\Software\ Altus\PassfiltProClient\targetDC, REG_SZ	Forces the client to use a specific DC for the rules. Typically it uses the DC specified by the %logonserver% variable. This works well if you are testing an only have nFront Password Filter installed on 1 DC in a domain with many DCs. Do not include '\\' in targetDC value.

2.7 FAQ

- Does the installation require a reboot? No.
- How can I tell it is installed or confirm the version I am running? It will display in Control Panel + Add/Remove Programs. You can click on the link marked “click here for support information” and a small dialog box with the version will be displayed.

3.0 The User Experience

When the user visits the site URL they will see this initial page.

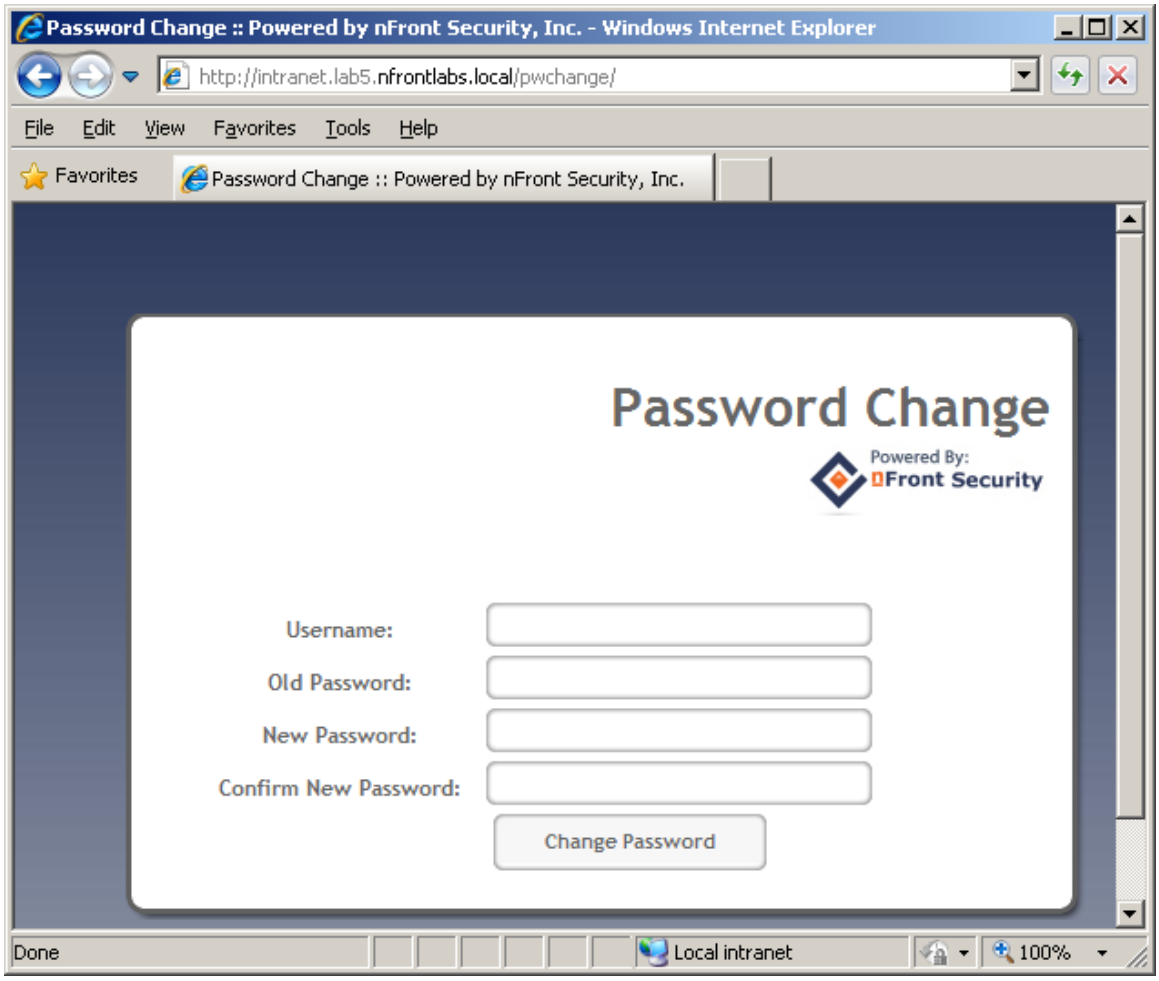


Figure 3.1: The initial screen.

After typing in a username (and tabbing to another text box or hitting enter) the page will dynamically refresh and display the list of password requirements.

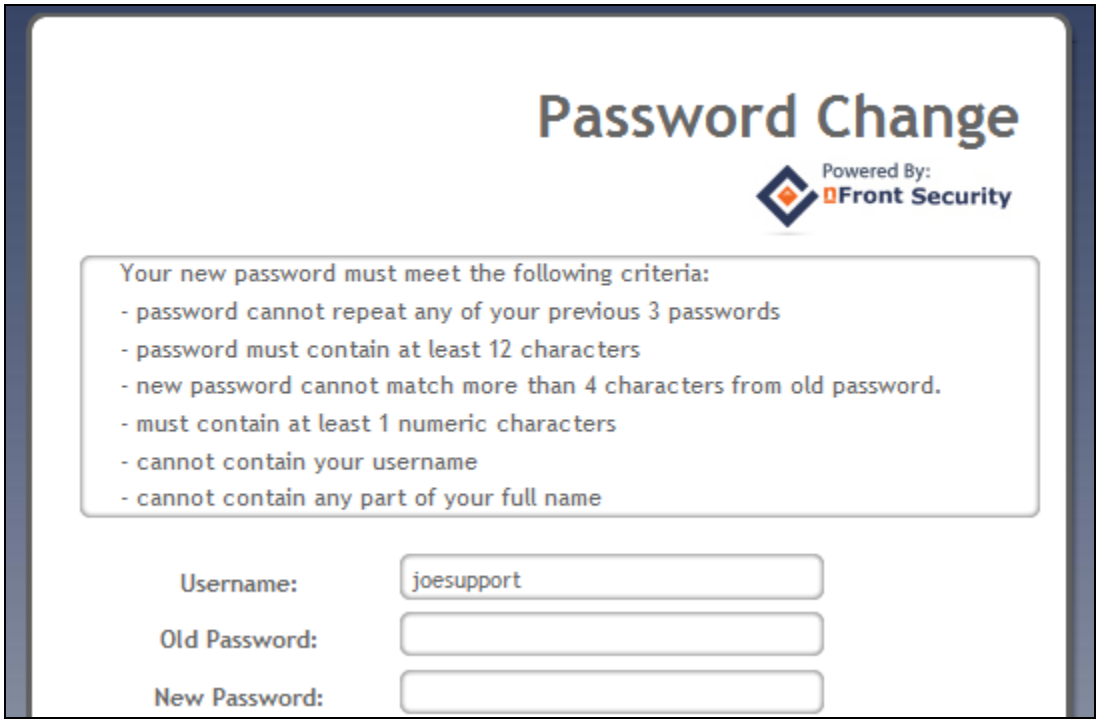


Figure 3.2: The rules are displayed after you enter your username

After filling in the fields the user can press the Change Password button or the Test Password button if you have enabled it (see Section 2.6 on customization).

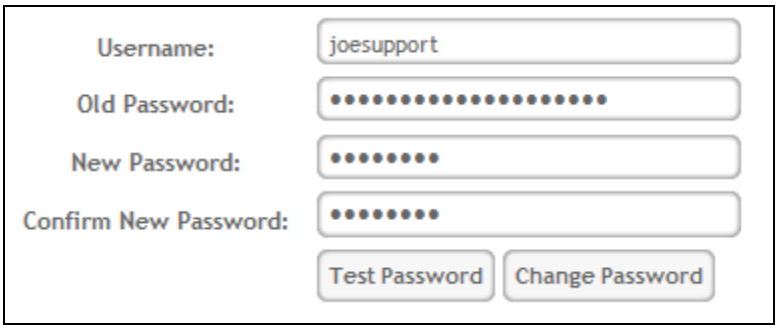


Figure 3.3: A Test Password button can be displayed.

If the new password fails any of the nFront password rules the reasons for failure are returned and appear in an orange font above the rules.

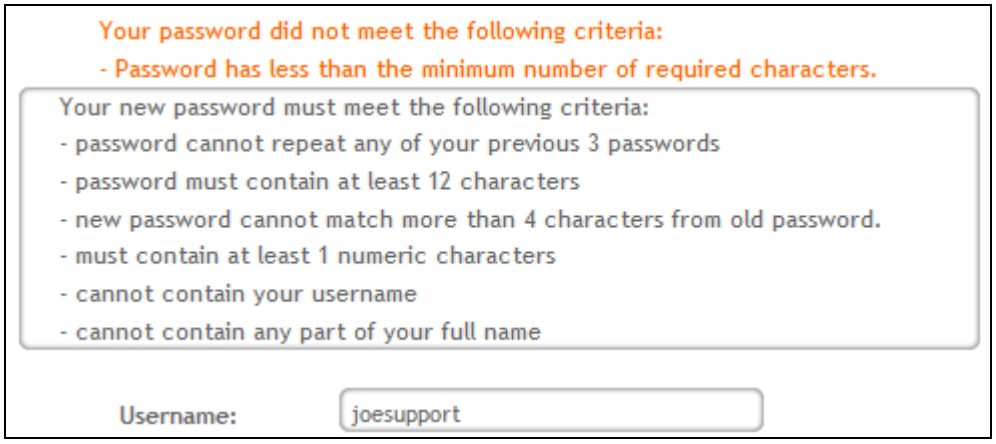


Figure 3.4: Failure messages are posted above the rules.

If the password change is successful, a “Password Change was Successful” message will be displayed. You may also send the user to another web page by adding a “successURL” value to the registry of the web server. See section 2.6 on customization.

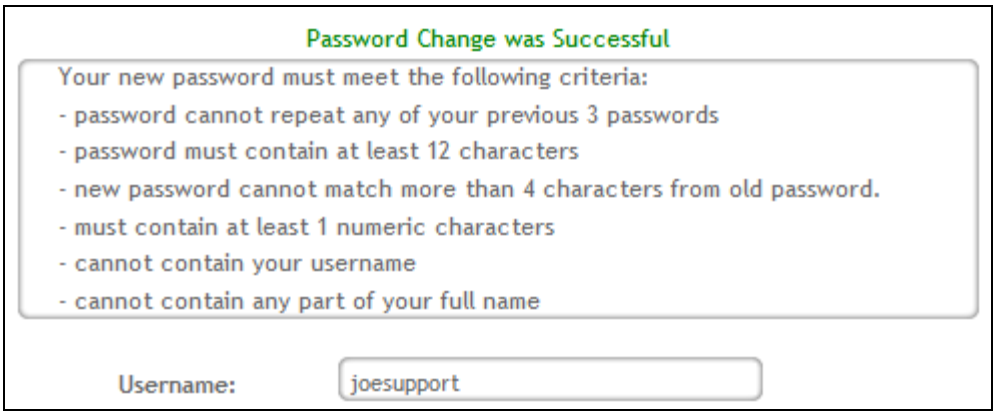


Figure 3.5: Example of a successful password change.

If you have turned on debugging (see section 2.6), the error code will be displayed just below the status message. In this case the error is zero because the change was successful. The nFront Web Password Change captures most errors and returns the correct text to the end user. For example, if the old password is incorrect the new password may meet the nFront rules but the password change will not be successful. In such case we trap the error for the incorrect old password and tell the user the old password is not correct.

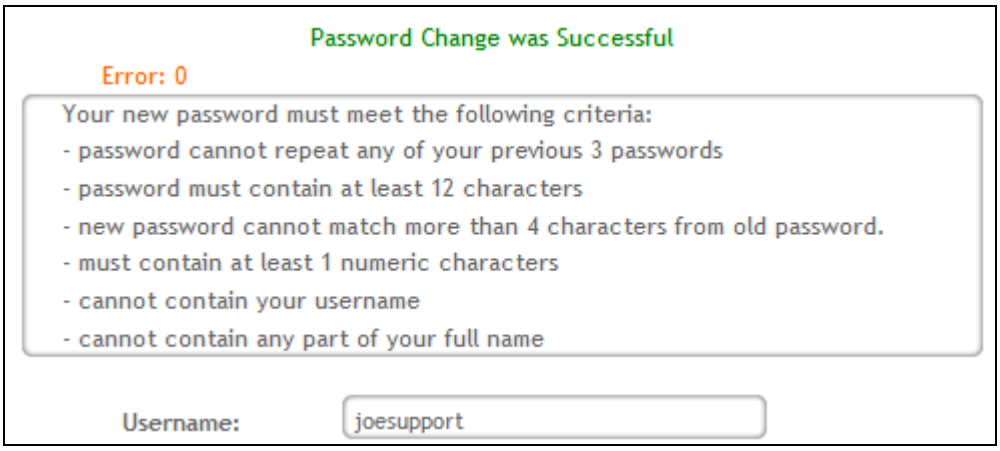


Figure 3.6: Password change with debugging turned on.

4.0 Registering your evaluation copy

The evaluation copy will display a red text message above the password rules and username field. The message is not displayed on a licensed copy.

Figure 4.1: Example of evaluation version.

After purchasing your license you will receive an email with a registration code. Go to Start + All Programs + nFront Web Password Change + Registration. Enter your new registration code and the software will no longer display the licensing message when clients connect.

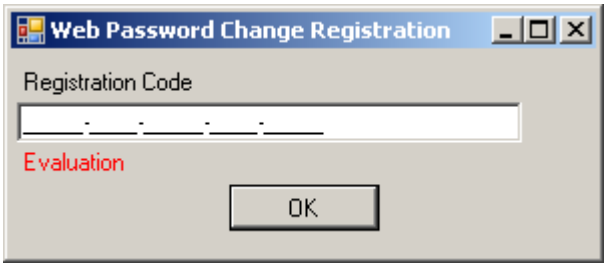


Figure 4.2: Registration dialog box.

5.0 Uninstall nFront Web Password Change

Control Panel + Programs + select nFront Web Password Change + uninstall.

Appendix A - nFront Web Password Change Debug Codes

Since the IIS application is running under the security context of the user sending debug information to a log file is not possible (without security concerns regarding users creating files on the IIS server). When the user clicks the Change Password Button we connect to the nFront Password Policy service on a domain controller to validate the password against nFront rules. If the password meets nFront requirements the regular Microsoft password change process is invoked and we attempt to trap any error codes returned.

Below is a list of error codes we trap. If you turn on debugging

Code	Error Displayed
5	Your account settings do not allow you to change your password.
86	Your old password is not correct."
1331	User account disabled.");
2245	Your new password has been used before or is less than the minimum password age.

Here are others we have encountered but do not trap. Since we do not trap these codes you will see a message on the screen that says “Your password does not meet the requirements” but no requirements will be listed. If you turn on debugging you will see the codes below.

Code	Reason
1351	This error is encountered when the web page is displayed via anonymous authentication. The virtual directory for the application should have authentication configure for : Anonymous Authentication: Disabled ASP.NET Impersonation: Enabled Windows Authentication: Enabled
2221	We have seen this error when the IIS app is in one domain and a user logged into another trusted domain in the forest goes to the web page. It occurs because the IIS process is doing impersonation using the trusted user from another domain. Since the app can only change passwords in the local domain it cannot and will not work for any users whose account exist in another domain (trusted or not trusted). If the user in the trusted domain uses another browser like Firefox he or she will be prompted for a username and password. If a user in the same domain as the IIS app is supplied the web page will allow a password change for that user.