nFront Security
Where Security & Solutions Intersect™

nFront Web Password Change

Version 3.4.0

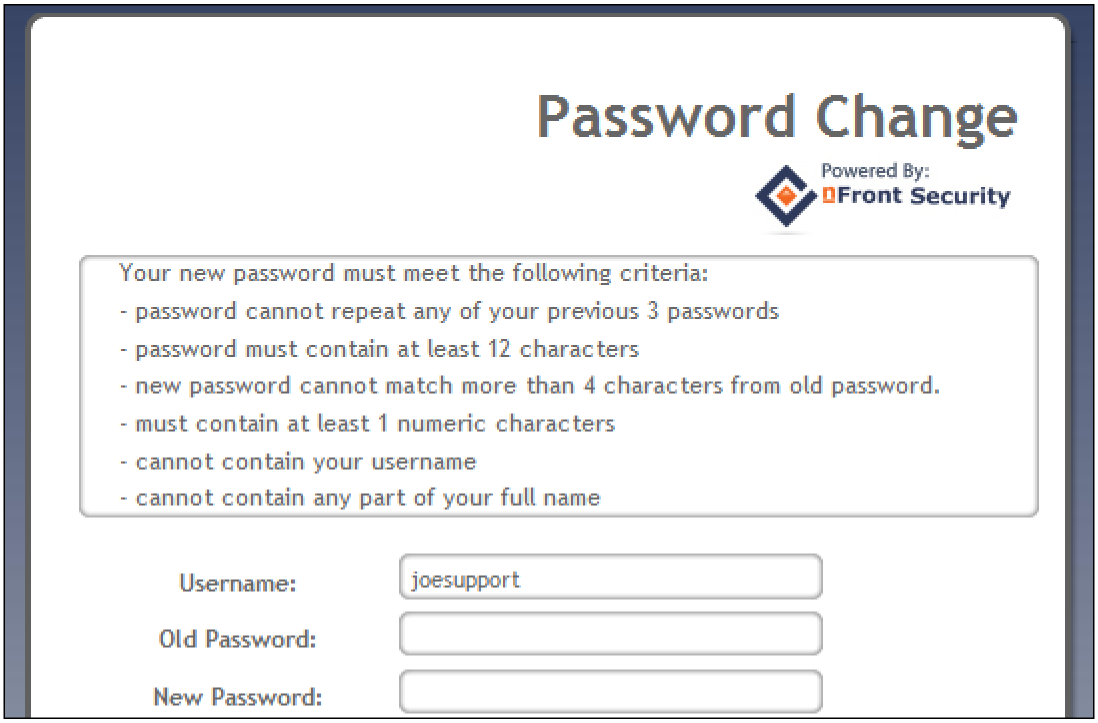
Documentation

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.



Your new password must meet the following criteria:
- password cannot repeat any of your previous 3 passwords
- password must contain at least 12 characters
- new password cannot match more than 4 characters from old password.
- must contain at least 1 numeric characters
- cannot contain your username
- cannot contain any part of your full name

Username: joesupport

Old Password:

New Password:

1.1 Requirements:

- Windows Server 2008, 2012, 2016 (R2 versions supported). 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 3.4?

- Installer has been updated to better work with all platforms (Windows 2008, 2012, 2016)
- Installer eliminates most post configuration steps required in prior versions.

What is new in Version 3.2?

- Supports modifying the language for the rules and failure message.

What is new in Version 3.1?

- Modified code to show error codes (if an error occurs) without the need to turn on debugging

- Added error messages for error 1351 (if anonymous authentication is on and windows authentication is not enabled) and error 2221 (process running under credentials of trusted user outside of this domain).

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.

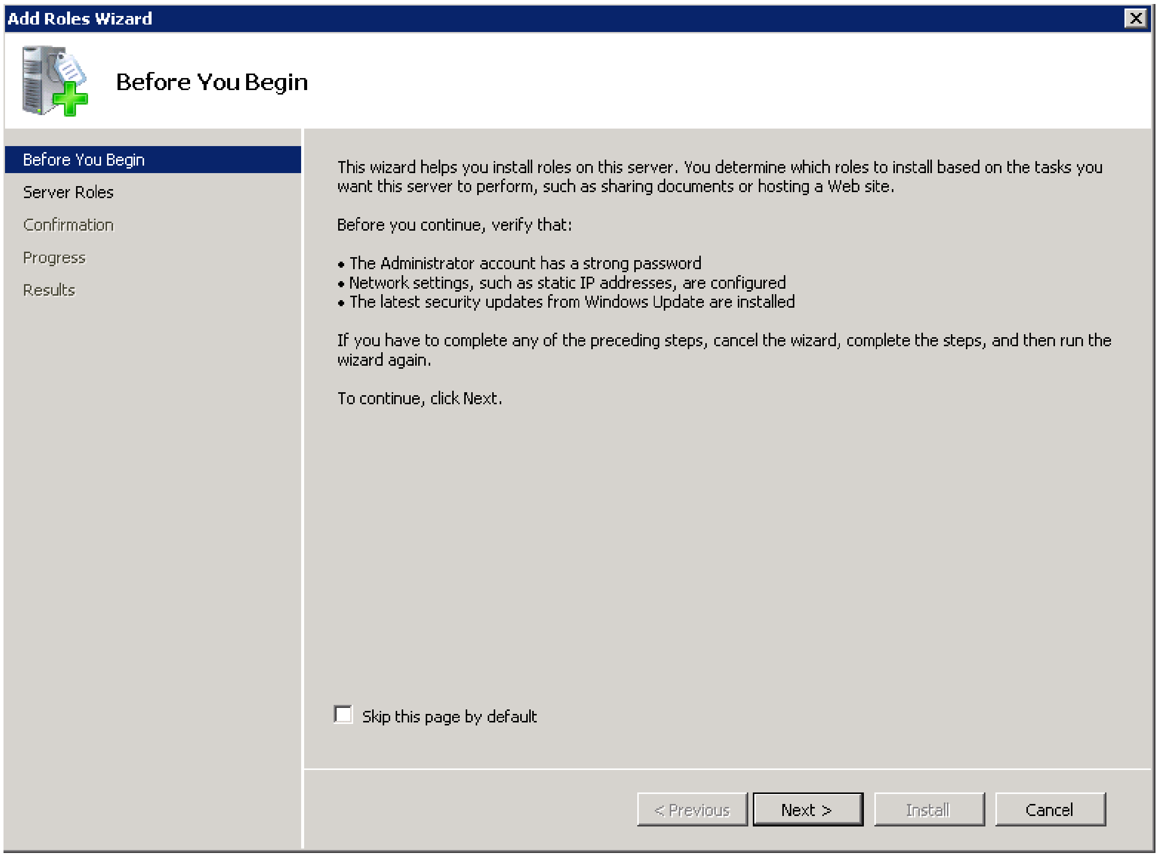
2.0 Installation

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.

In version 3.4.0 the software was packaged with a new installer that automates some post-configuration steps needed by prior versions.

Before running the installer, please make sure IIS is installed with the correct features. The remaining sections will cover the installation on Windows 2008 R2, Windows 2012 R2 and Server 2016. Please refer to the instructions for your specific OS.

2.1 Installation on Windows 2008 R2



This wizard helps you install roles on this server. You determine which roles to install based on the tasks you want this server to perform, such as sharing documents or hosting a Web site.

Before you continue, verify that:

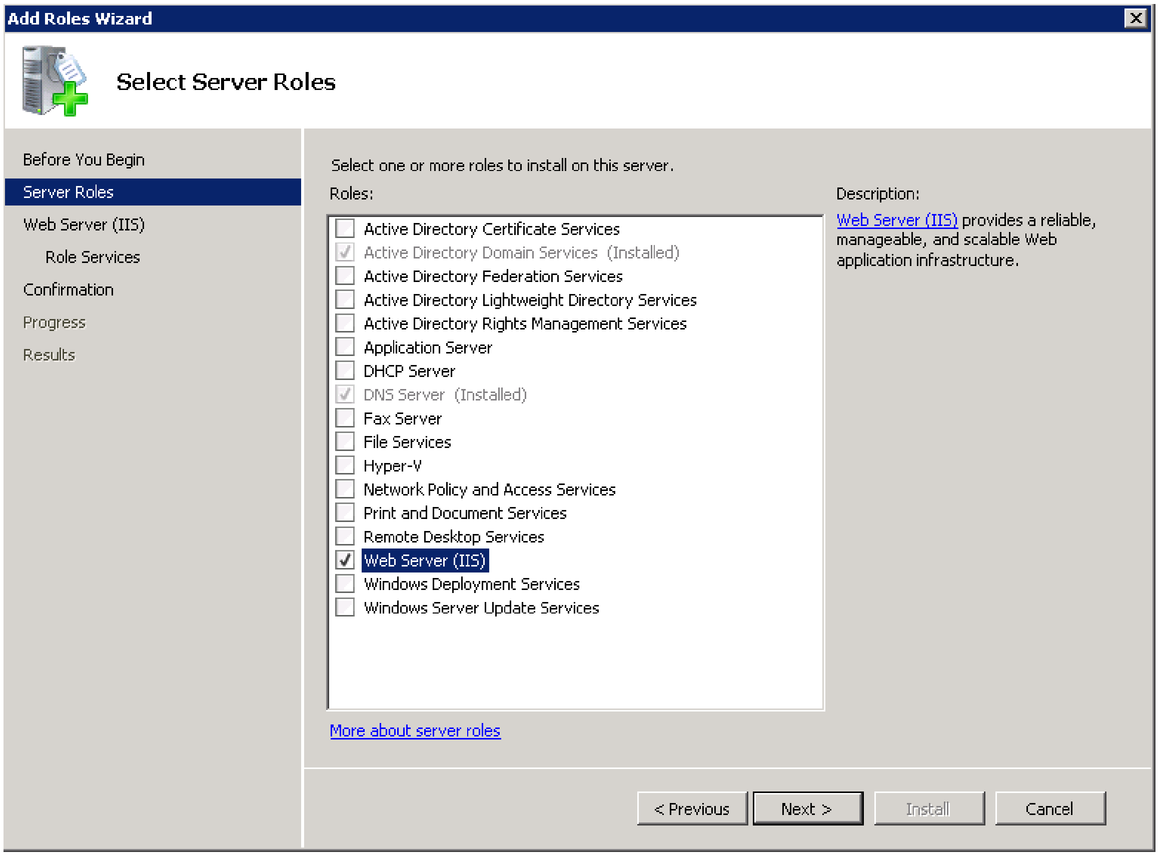
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The latest security updates from Windows Update are installed

If you have to complete any of the preceding steps, cancel the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

☐ Skip this page by default

Figure 2.1.1 – Adding Web Server (IIS) Role on Windows 2008 R2



Select one or more roles to install on this server.

Roles:

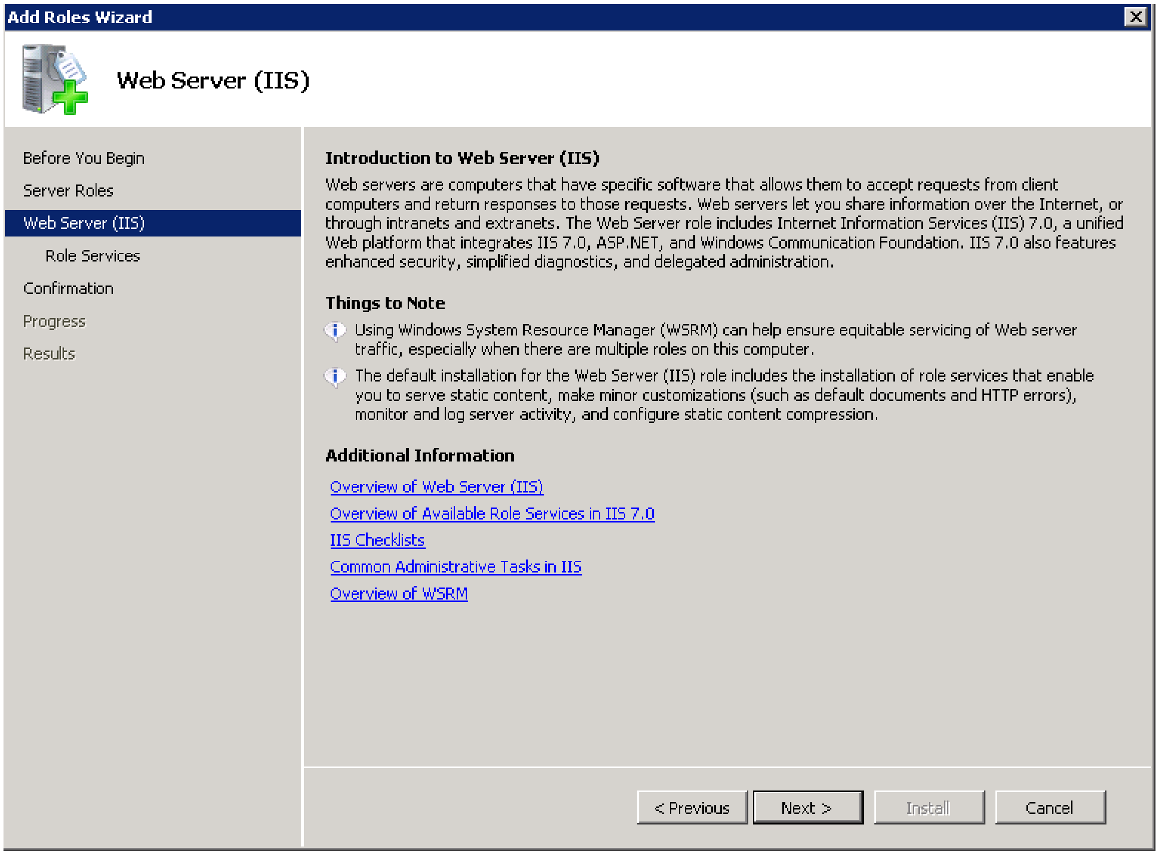
- ☐ Active Directory Certificate Services
- ☑ Active Directory Domain Services (Installed)
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☑ DNS Server (Installed)
- ☐ Fax Server
- ☐ File Services
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Desktop Services
- ☑ Web Server (IIS)
- ☐ Windows Deployment Services
- ☐ Windows Server Update Services

Description:

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

More about server roles

Figure 2.1.2 –Windows 2008 R2 Add Roles Wizard Step 2



Introduction to Web Server (IIS)

Web servers are computers that have specific software that allows them to accept requests from client computers and return responses to those requests. Web servers let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 7.0, a unified Web platform that integrates IIS 7.0, ASP.NET, and Windows Communication Foundation. IIS 7.0 also features enhanced security, simplified diagnostics, and delegated administration.

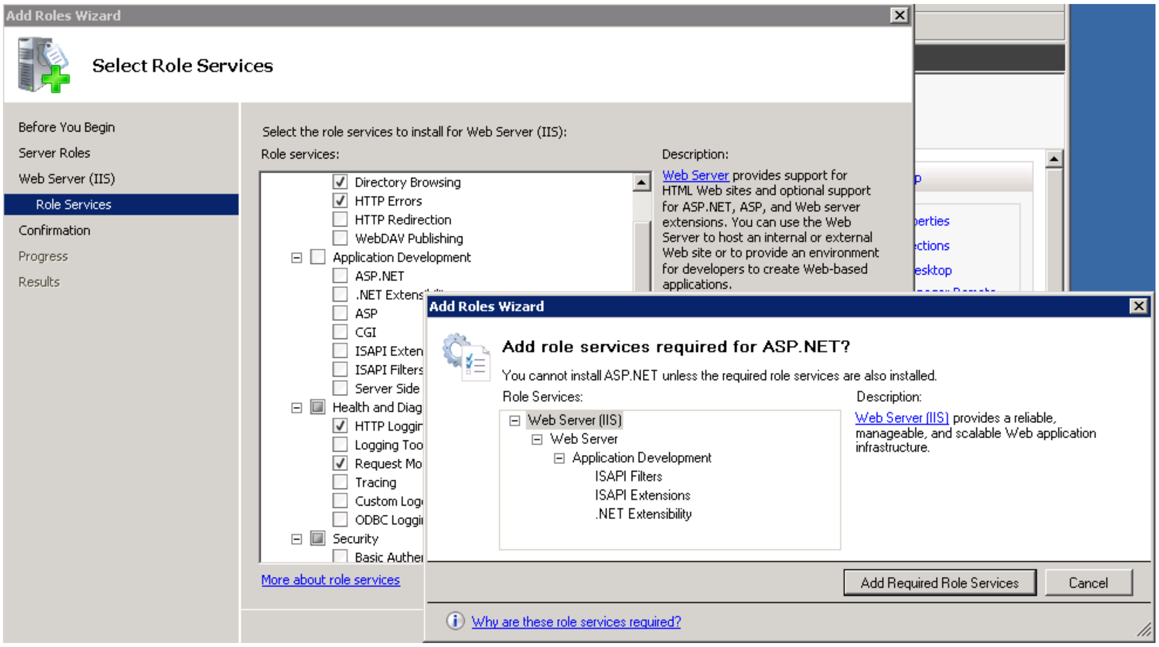
Things to Note

- Using Windows System Resource Manager (WSRM) can help ensure equitable servicing of Web server traffic, especially when there are multiple roles on this computer.
- The default installation for the Web Server (IIS) role includes the installation of role services that enable you to serve static content, make minor customizations (such as default documents and HTTP errors), monitor and log server activity, and configure static content compression.

Additional Information

Overview of Web Server (IIS)
Overview of Available Role Services in IIS 7.0
IIS Checklists
Common Administrative Tasks in IIS
Overview of WSRM

Figure 2.1.3 –Windows 2008 R2 Add Roles Wizard Step 3



Select the role services to install for Web Server (IIS):

Role services:

☑ Directory Browsing
☑ HTTP Errors
□ HTTP Redirection
□ WebDAV Publishing
□ Application Development
□ ASP.NET
□ .NET Extens
□ ASP
□ CGI
□ ISAPI Exten
□ ISAPI Filters
□ Server Side
▣ Health and Diag
☑ HTTP Loggir
□ Logging Too
☑ Request Mo
□ Tracing
□ Custom Log
□ ODBC Loggi
▣ Security
□ Basic Authe

More about role services

Description:

Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.

Add role services required for ASP.NET?

You cannot install ASP.NET unless the required role services are also installed.

Role Services:

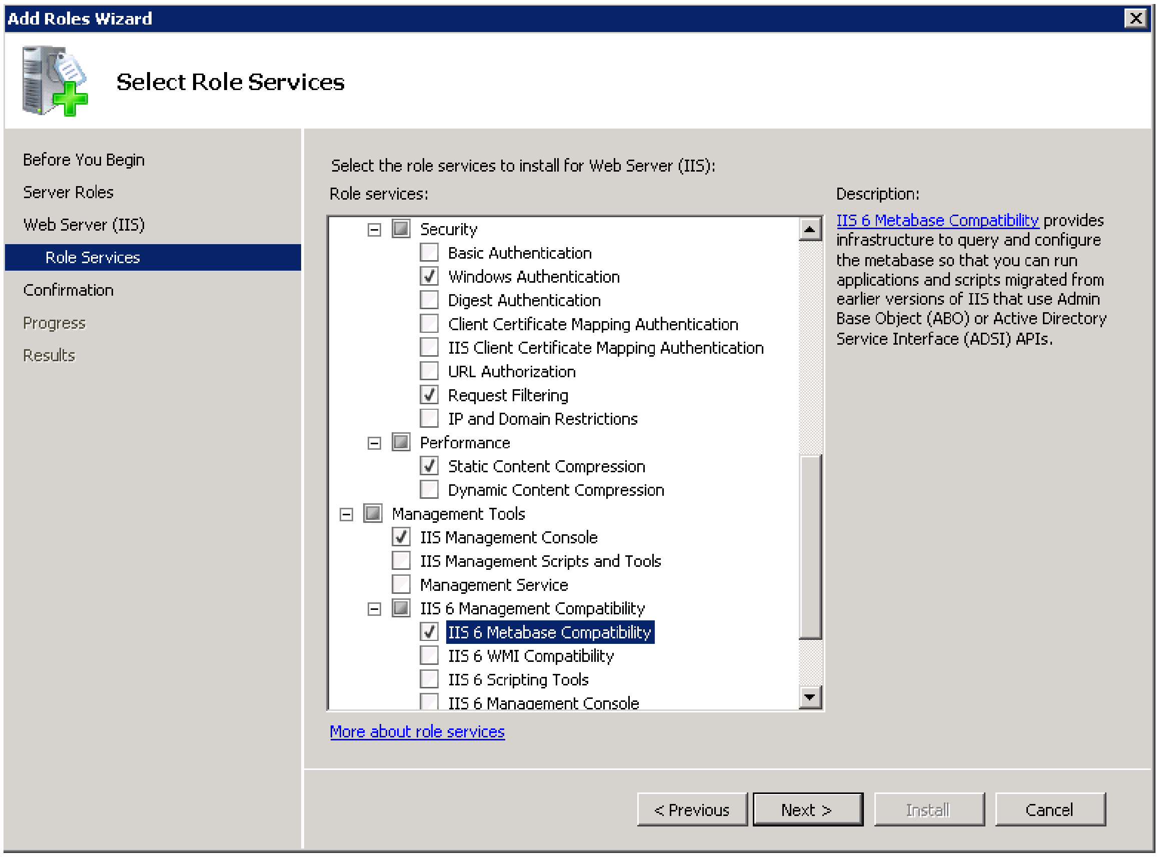
```
⊟ Web Server (IIS)
    ⊟ Web Server
        ⊟ Application Development
              ISAPI Filters
              ISAPI Extensions
              .NET Extensibility
```

Description:

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

Why are these role services required?

Figure 2.1.4 –Windows 2008 R2 Add Roles Wizard Step 4



Select Role Services

Select the role services to install for Web Server (IIS):

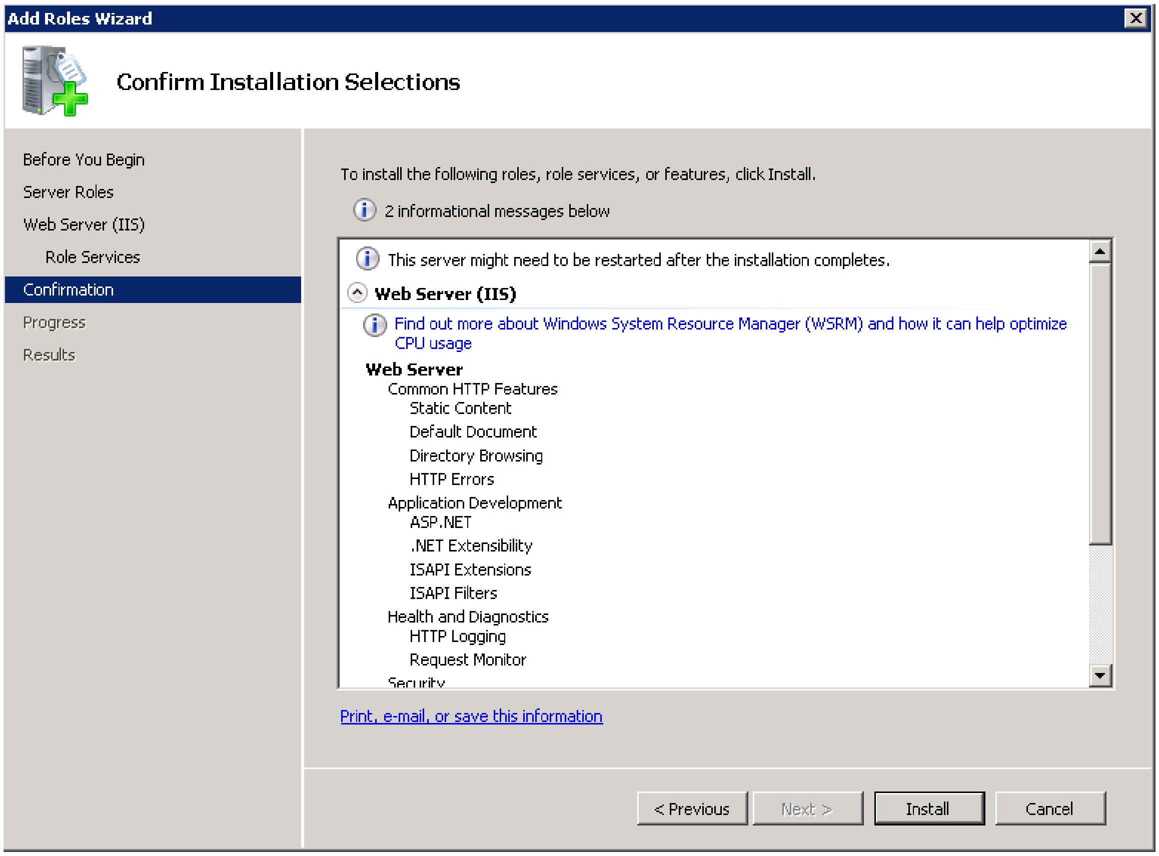
Role services:

- ▣ Security
  - □ Basic Authentication
  - ☑ Windows Authentication
  - □ Digest Authentication
  - □ Client Certificate Mapping Authentication
  - □ IIS Client Certificate Mapping Authentication
  - □ URL Authorization
  - ☑ Request Filtering
  - □ IP and Domain Restrictions
- ▣ Performance
  - ☑ Static Content Compression
  - □ Dynamic Content Compression
- ▣ Management Tools
  - ☑ IIS Management Console
  - □ IIS Management Scripts and Tools
  - □ Management Service
  - ▣ IIS 6 Management Compatibility
    - ☑ IIS 6 Metabase Compatibility
    - □ IIS 6 WMI Compatibility
    - □ IIS 6 Scripting Tools
    - □ IIS 6 Management Console

Description:

IIS 6 Metabase Compatibility provides infrastructure to query and configure the metabase so that you can run applications and scripts migrated from earlier versions of IIS that use Admin Base Object (ABO) or Active Directory Service Interface (ADSI) APIs.

Figure 2.1.5 –Windows 2008 R2 Add Roles Wizard Step 5



Add Roles Wizard

Confirm Installation Selections

To install the following roles, role services, or features, click Install.

2 informational messages below

This server might need to be restarted after the installation completes.

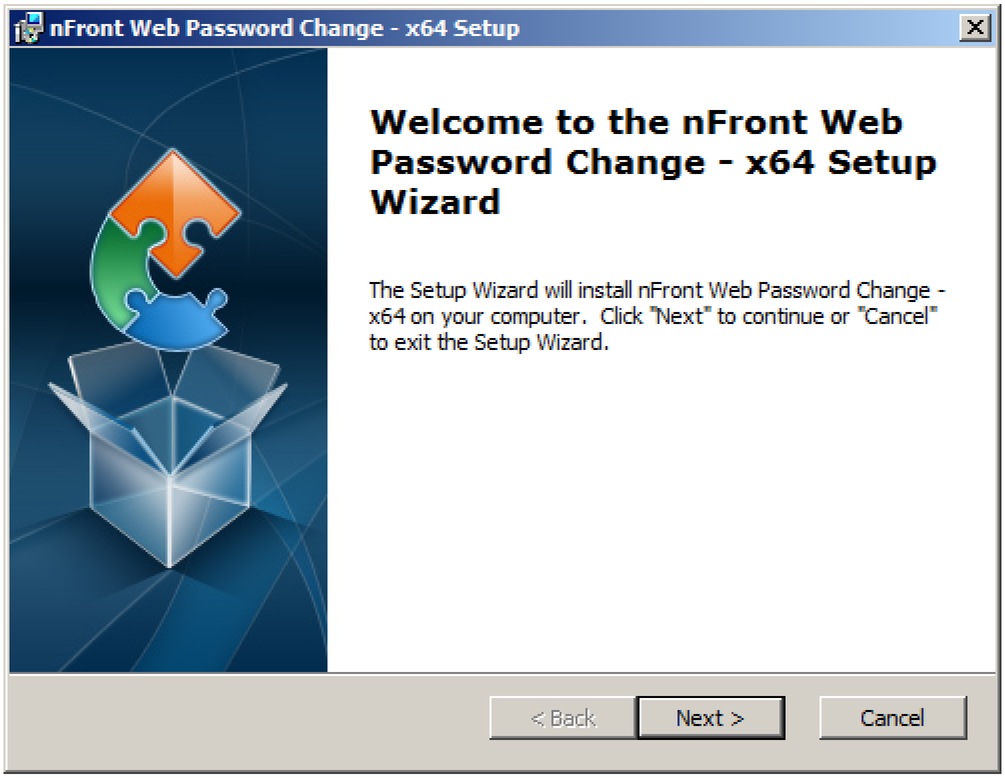
Web Server (IIS)

Find out more about Windows System Resource Manager (WSRM) and how it can help optimize CPU usage

Web Server
  Common HTTP Features
    Static Content
    Default Document
    Directory Browsing
    HTTP Errors
  Application Development
    ASP.NET
    .NET Extensibility
    ISAPI Extensions
    ISAPI Filters
  Health and Diagnostics
    HTTP Logging
    Request Monitor
  Security

Print, e-mail, or save this information

Figure 2.1.6 –Windows 2008 R2 Add Roles Wizard Step 6

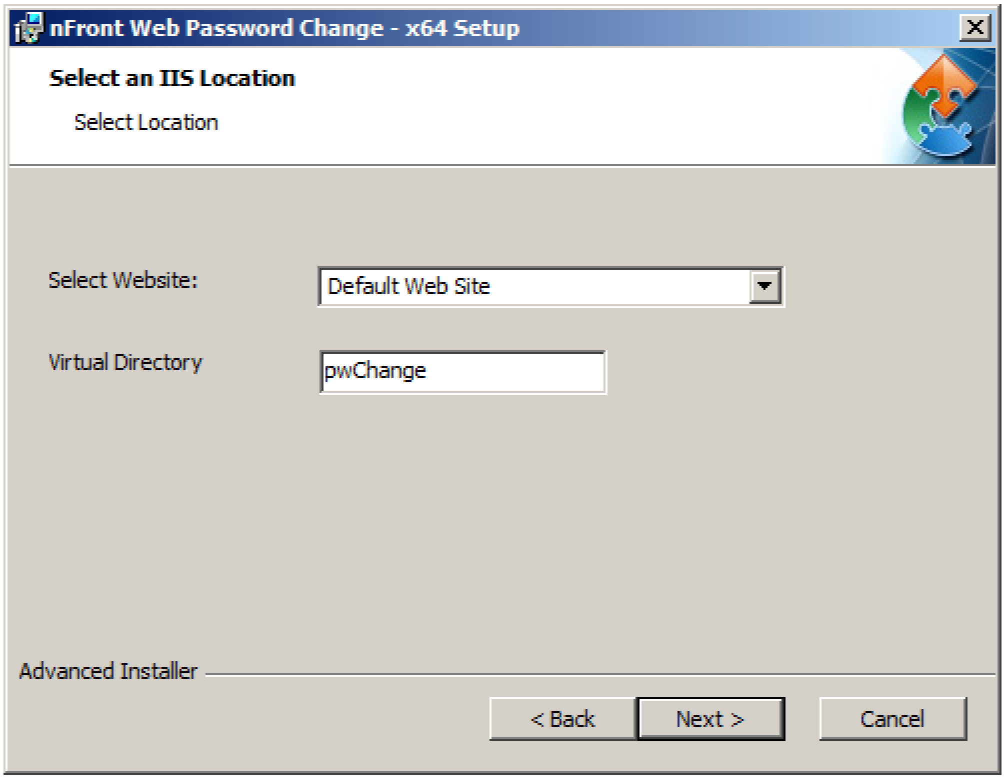


nFront Web Password Change - x64 Setup

Welcome to the nFront Web Password Change - x64 Setup Wizard

The Setup Wizard will install nFront Web Password Change - x64 on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

Figure 2.1.7 –NPF-WEB Installer – Step 1



nFront Web Password Change - x64 Setup

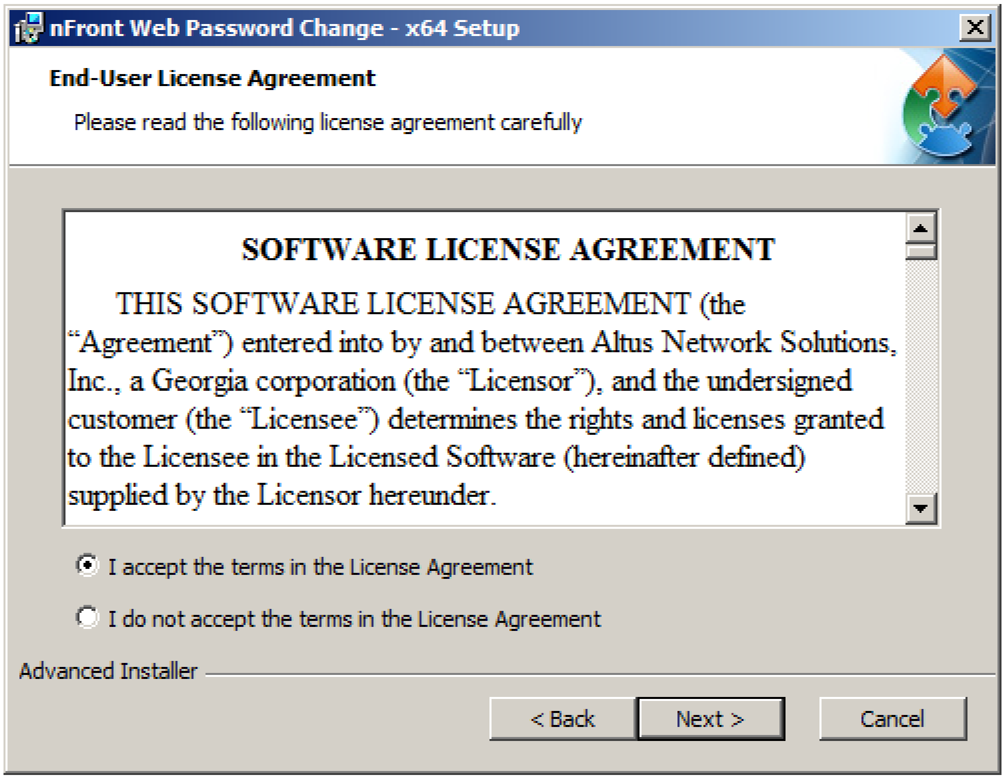
Select an IIS Location

Select Location

Select Website: Default Web Site

Virtual Directory pwChange

Figure 2.1.8 –NPF-WEB Installer – Step 2



End-User License Agreement

Please read the following license agreement carefully

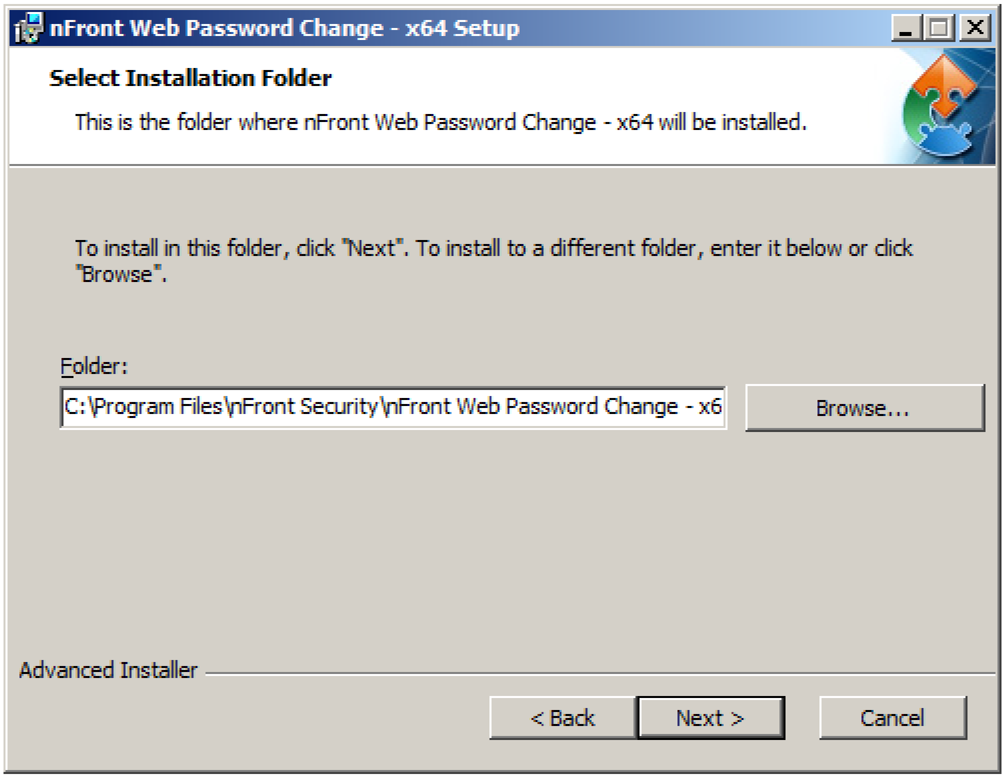
SOFTWARE LICENSE AGREEMENT

THIS SOFTWARE LICENSE AGREEMENT (the "Agreement") entered into by and between Altus Network Solutions, Inc., a Georgia corporation (the "Licensor"), and the undersigned customer (the "Licensee") determines the rights and licenses granted to the Licensee in the Licensed Software (hereinafter defined) supplied by the Licensor hereunder.

● I accept the terms in the License Agreement

○ I do not accept the terms in the License Agreement

Figure 2.1.9 –NPF-WEB Installer – Step 3


nFront Web Password Change - x64 Setup

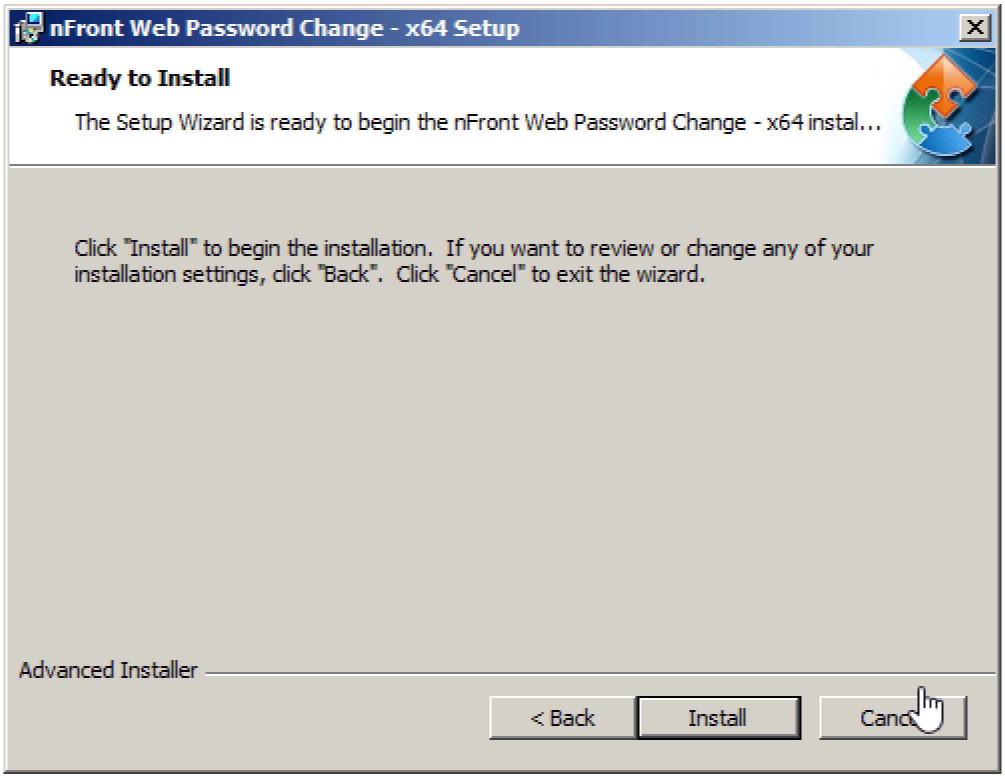
Select Installation Folder

This is the folder where nFront Web Password Change - x64 will be installed.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files\nFront Security\nFront Web Password Change - x6

Figure 2.1.10 –NPF-WEB Installer – Step 4

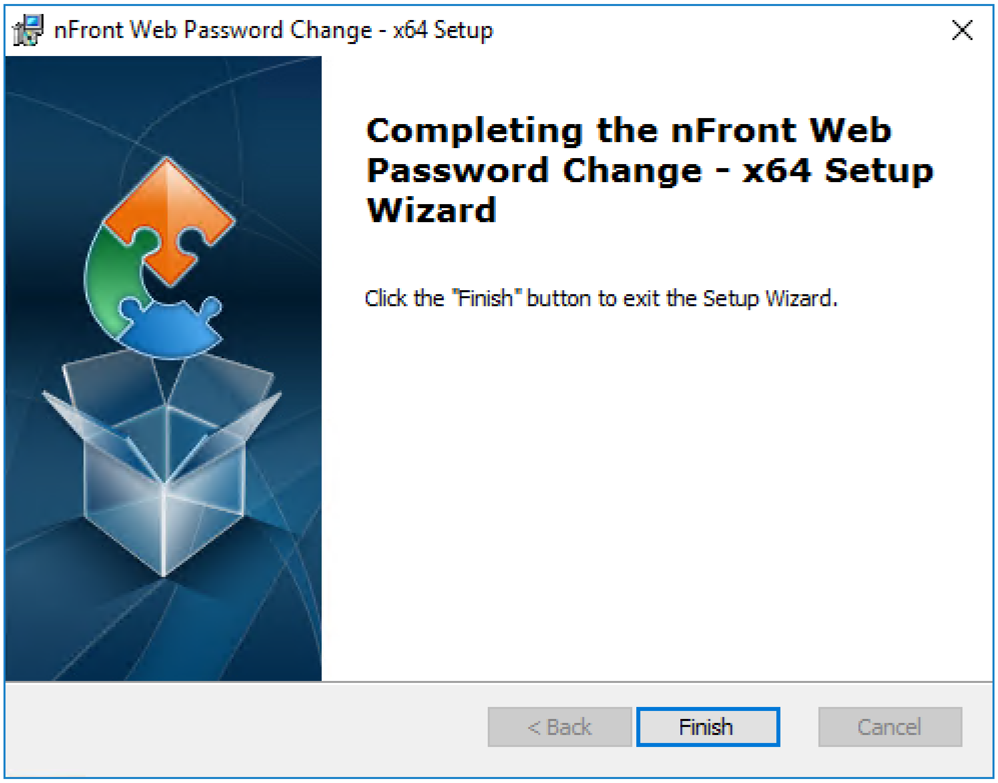

nFront Web Password Change - x64 Setup

Ready to Install

The Setup Wizard is ready to begin the nFront Web Password Change - x64 instal...

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

Figure 2.1.11 –NPF-WEB Installer – Step 5

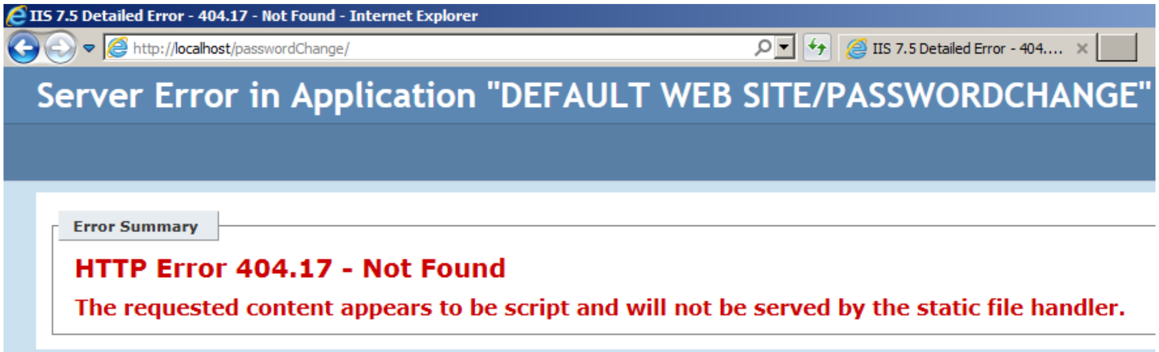


Completing the nFront Web Password Change - x64 Setup Wizard

Click the "Finish" button to exit the Setup Wizard.

Figure 2.1.12 –NPF-WEB Installer – Step 6

If you test at this point you will get error 404.17. You will need to run a command line utility to install ASP.NET 4.0.



IIS 7.5 Detailed Error - 404.17 - Not Found - Internet Explorer
http://localhost/passwordChange/
IIS 7.5 Detailed Error - 404....

Server Error in Application "DEFAULT WEB SITE/PASSWORDCHANGE"

Error Summary

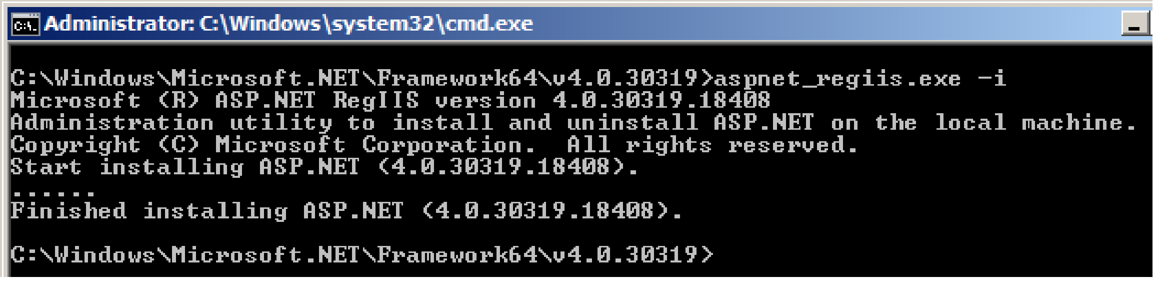
HTTP Error 404.17 - Not Found

The requested content appears to be script and will not be served by the static file handler.

Figure 2.1.13 – Application not working until you register ASP.NET 4

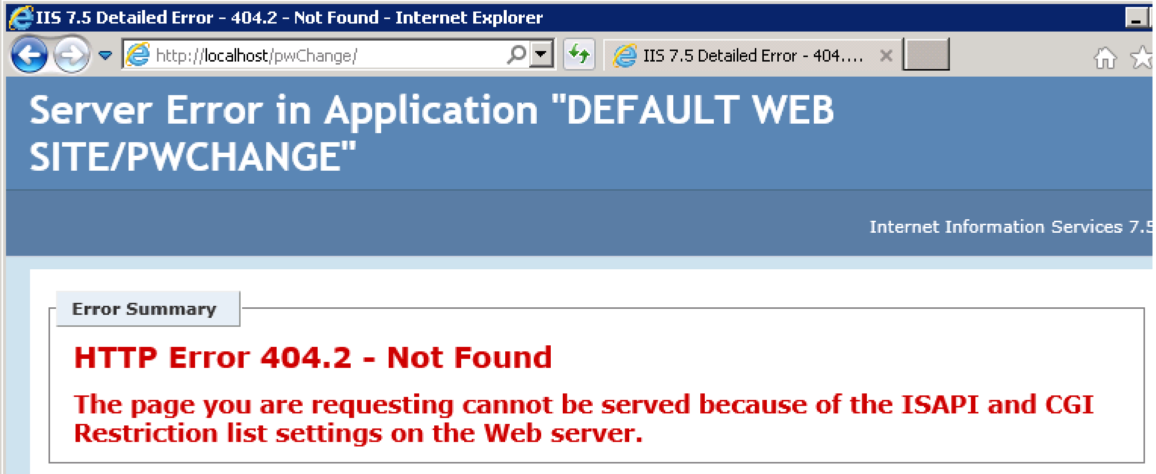
You will need to navigate to C:\Windows\Microsoft.NET\Framework64\v4.0.30319 and type the following command:

```
aspnet_regiis.exe -i
```



```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319>aspnet_regiis.exe -i
Microsoft (R) ASP.NET RegIIS version 4.0.30319.18408
Administration utility to install and uninstall ASP.NET on the local machine.
Copyright (C) Microsoft Corporation.  All rights reserved.
Start installing ASP.NET (4.0.30319.18408).
......
Finished installing ASP.NET (4.0.30319.18408).

C:\Windows\Microsoft.NET\Framework64\v4.0.30319>
```

Figure 2.1.14 – Registering ASP.NET 4


IIS 7.5 Detailed Error - 404.2 - Not Found - Internet Explorer
http://localhost/pwChange/
IIS 7.5 Detailed Error - 404....
Internet Information Services 7.5
Error Summary

Server Error in Application "DEFAULT WEB SITE/PWCHANGE"

HTTP Error 404.2 - Not Found

The page you are requesting cannot be served because of the ISAPI and CGI Restriction list settings on the Web server.

Figure 2.1.15 – The application will still not work until ISAPI and CGI settings are changed

In the IIS Manager, select the server in the left pane, and double click ISAPI and CGI Restrictions in the right pane.

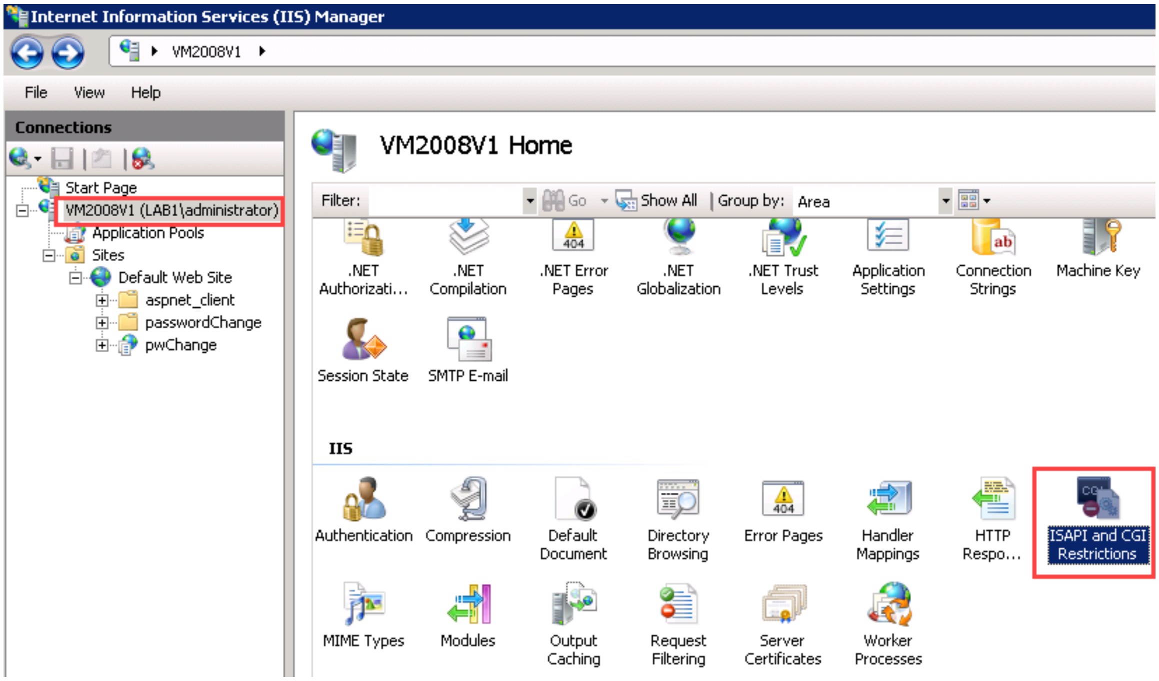
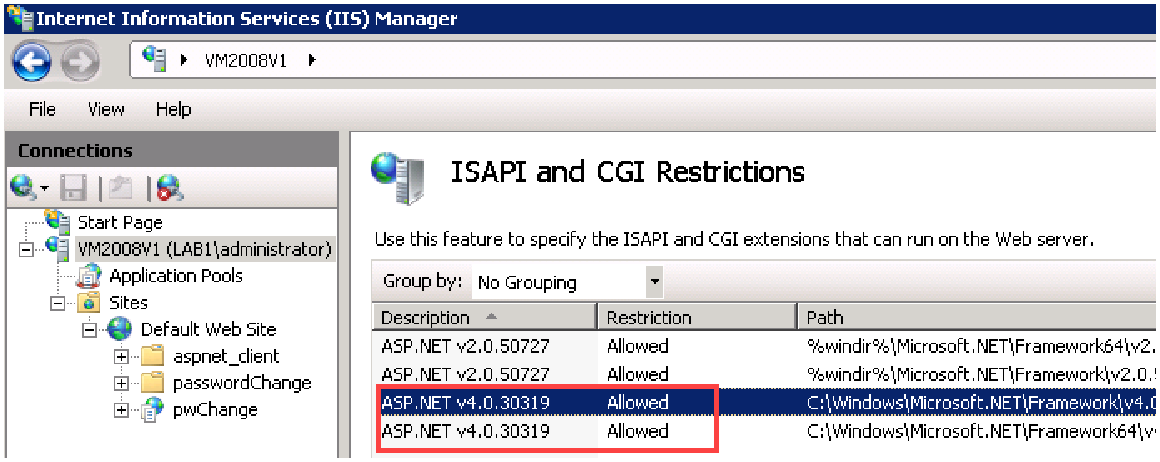


Figure 2.1.16 – Select ISAPI and CGI Restrictions

Right click ASP.NET v4.0.303319 for both Framework64 and select Allowed. Do the same for the Framework entry.



ISAPI and CGI Restrictions

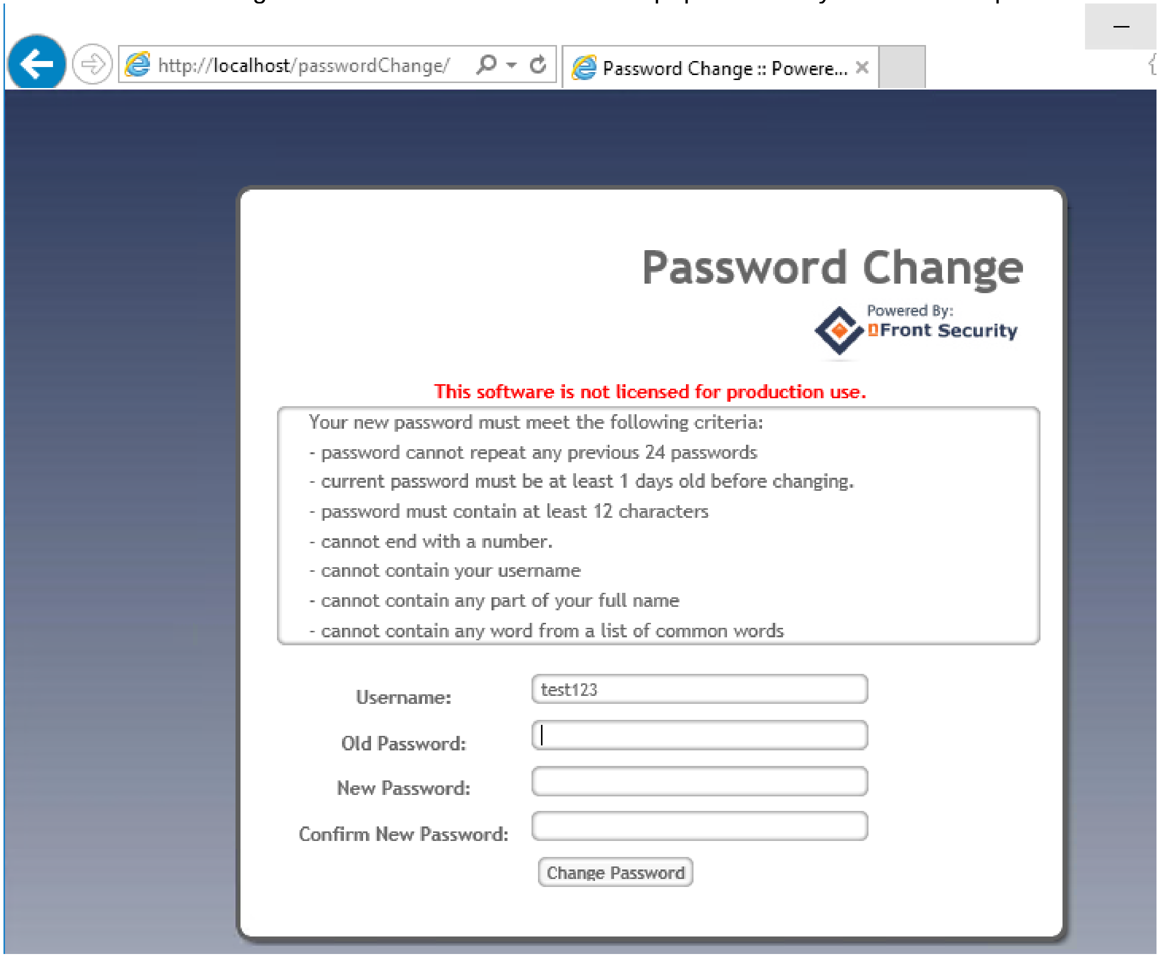
Use this feature to specify the ISAPI and CGI extensions that can run on the Web server.

Group by: No Grouping

Description	Restriction	Path
ASP.NET v2.0.50727	Allowed	%windir%\Microsoft.NET\Framework64\v2.
ASP.NET v2.0.50727	Allowed	%windir%\Microsoft.NET\Framework\v2.0.!
ASP.NET v4.0.30319	Allowed	C:\Windows\Microsoft.NET\Framework\v4.(
ASP.NET v4.0.30319	Allowed	C:\Windows\Microsoft.NET\Framework64\v·

Figure 2.1.17 – Allow ISAPI and CGI for ASP.NET v4

Now a test of http://localhost/passwordChange should work as expected. After tying in a username and moving to another field the rules should populate with your nFront requirements.


http://localhost/passwordChange/
Password Change :: Powere...
Password Change
Powered By:
nFront Security

This software is not licensed for production use.

Your new password must meet the following criteria:
- password cannot repeat any previous 24 passwords
- current password must be at least 1 days old before changing.
- password must contain at least 12 characters
- cannot end with a number.
- cannot contain your username
- cannot contain any part of your full name
- cannot contain any word from a list of common words

Username: test123

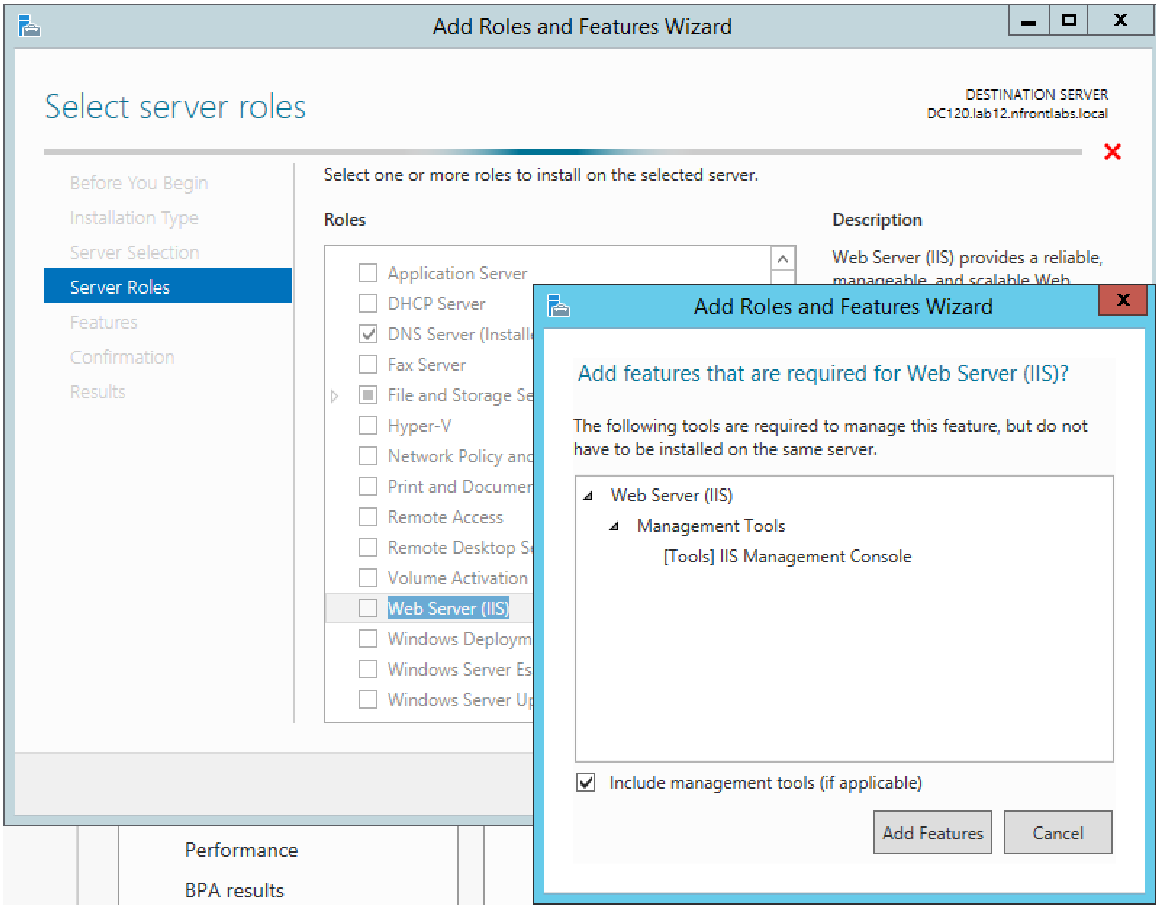
Old Password:

New Password:

Confirm New Password:

Figure 2.1.18 – NPF-WEB test on Windows 2008 R2

2.2 Installation on Windows 2012 R2



Select server roles

DESTINATION SERVER
DC120.lab12.nfrontlabs.local

Select one or more roles to install on the selected server.

Roles

- □ Application Server
- □ DHCP Server
- ☑ DNS Server (Install
- □ Fax Server
- ▨ File and Storage Se
- □ Hyper-V
- □ Network Policy and
- □ Print and Documen
- □ Remote Access
- □ Remote Desktop S
- □ Volume Activation
- □ Web Server (IIS)
- □ Windows Deploym
- □ Windows Server Es
- □ Windows Server U

Description

Web Server (IIS) provides a reliable, manageable, and scalable Web

Add Roles and Features Wizard

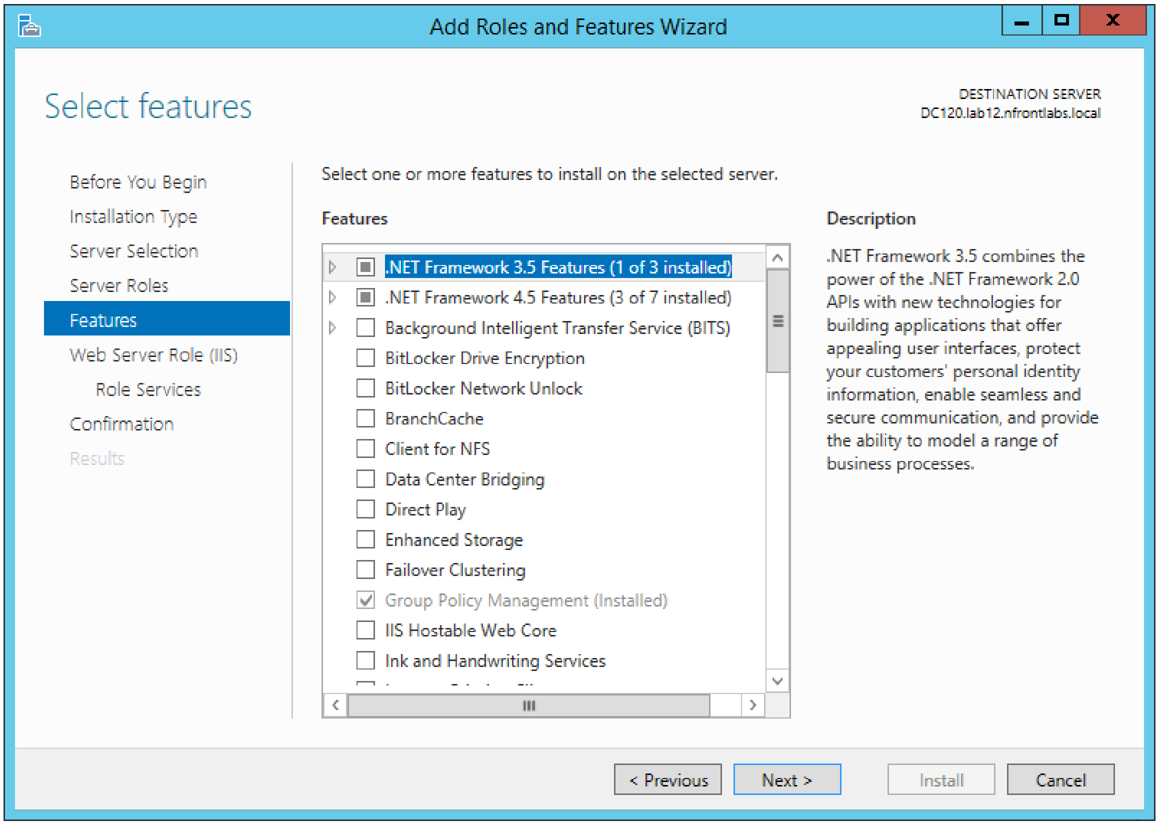
Add features that are required for Web Server (IIS)?

The following tools are required to manage this feature, but do not have to be installed on the same server.

- Web Server (IIS)
  - Management Tools
    - [Tools] IIS Management Console

☑ Include management tools (if applicable)

Figure 2.2.1 – Adding Web Server (IIS) Role on Windows 2012 R2



Select features

DESTINATION SERVER
DC120.lab12.nfrontlabs.local

Select one or more features to install on the selected server.

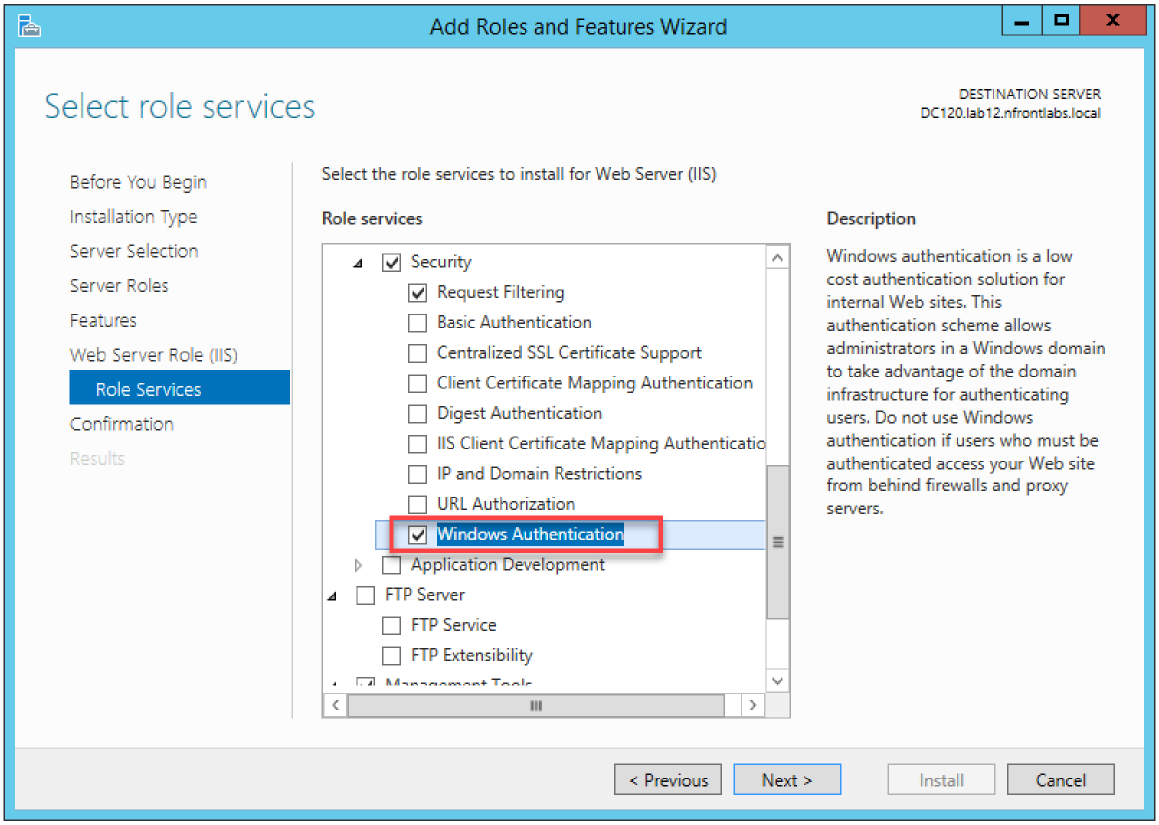
Features

- ▣ .NET Framework 3.5 Features (1 of 3 installed)
- ▣ .NET Framework 4.5 Features (3 of 7 installed)
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BitLocker Network Unlock
- □ BranchCache
- □ Client for NFS
- □ Data Center Bridging
- □ Direct Play
- □ Enhanced Storage
- □ Failover Clustering
- ☑ Group Policy Management (Installed)
- □ IIS Hostable Web Core
- □ Ink and Handwriting Services

Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

Figure 2.2.2 –Windows 2012 R2 Add Roles Wizard Step 2



Select role services

DESTINATION SERVER
DC120.lab12.nfrontlabs.local

Select the role services to install for Web Server (IIS)

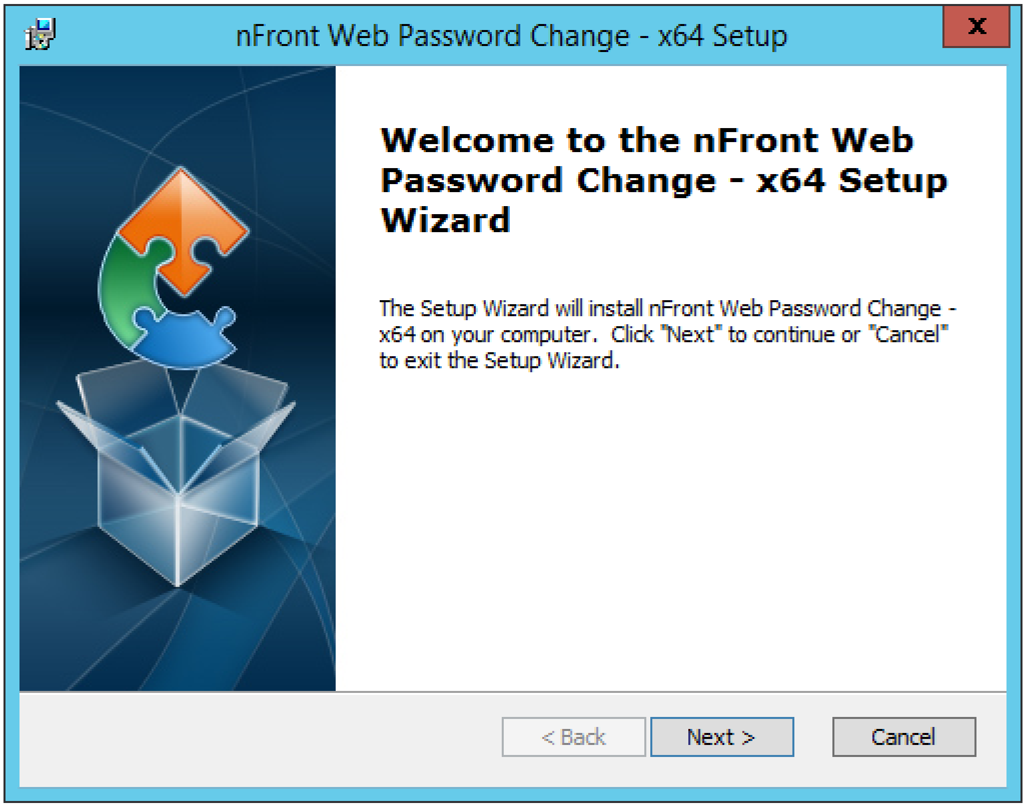
Role services

- ☑ Security
  - ☑ Request Filtering
  - ☐ Basic Authentication
  - ☐ Centralized SSL Certificate Support
  - ☐ Client Certificate Mapping Authentication
  - ☐ Digest Authentication
  - ☐ IIS Client Certificate Mapping Authenticatio
  - ☐ IP and Domain Restrictions
  - ☐ URL Authorization
  - ☑ Windows Authentication
- ☐ Application Development
- ☐ FTP Server
  - ☐ FTP Service
  - ☐ FTP Extensibility
- ☑ Management Tools

Description

Windows authentication is a low cost authentication solution for internal Web sites. This authentication scheme allows administrators in a Windows domain to take advantage of the domain infrastructure for authenticating users. Do not use Windows authentication if users who must be authenticated access your Web site from behind firewalls and proxy servers.

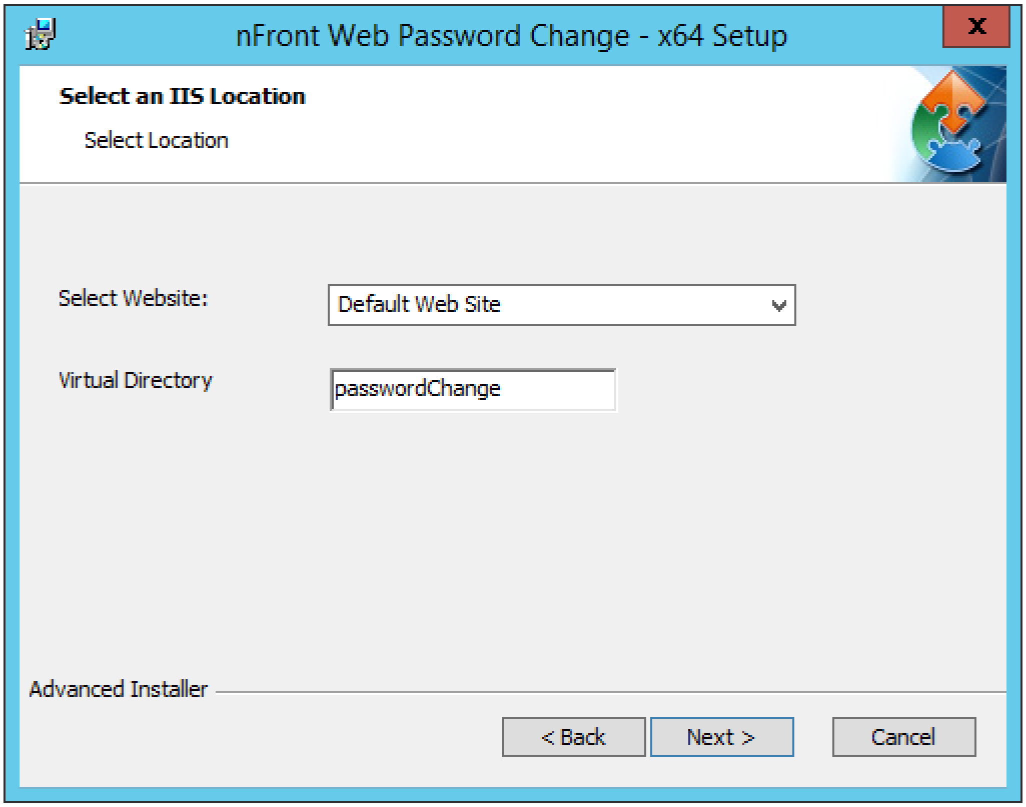
Figure 2.2.3 –Windows 2012 R2 Add Roles Wizard Step 3



Welcome to the nFront Web Password Change - x64 Setup Wizard

The Setup Wizard will install nFront Web Password Change - x64 on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

Figure 2.2.4 –NPF-WEB Installer – Step 1



nFront Web Password Change - x64 Setup

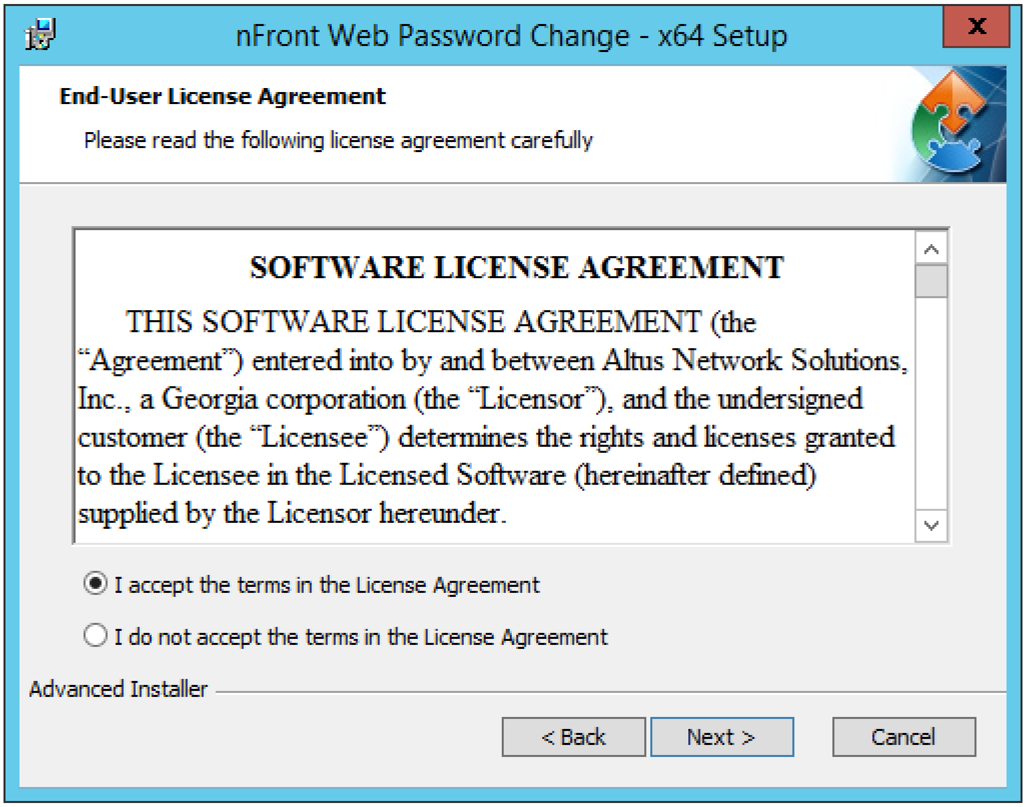
Select an IIS Location

Select Location

Select Website: Default Web Site

Virtual Directory passwordChange

Figure 2.2.5 –NPF-WEB Installer – Step 2



End-User License Agreement

Please read the following license agreement carefully

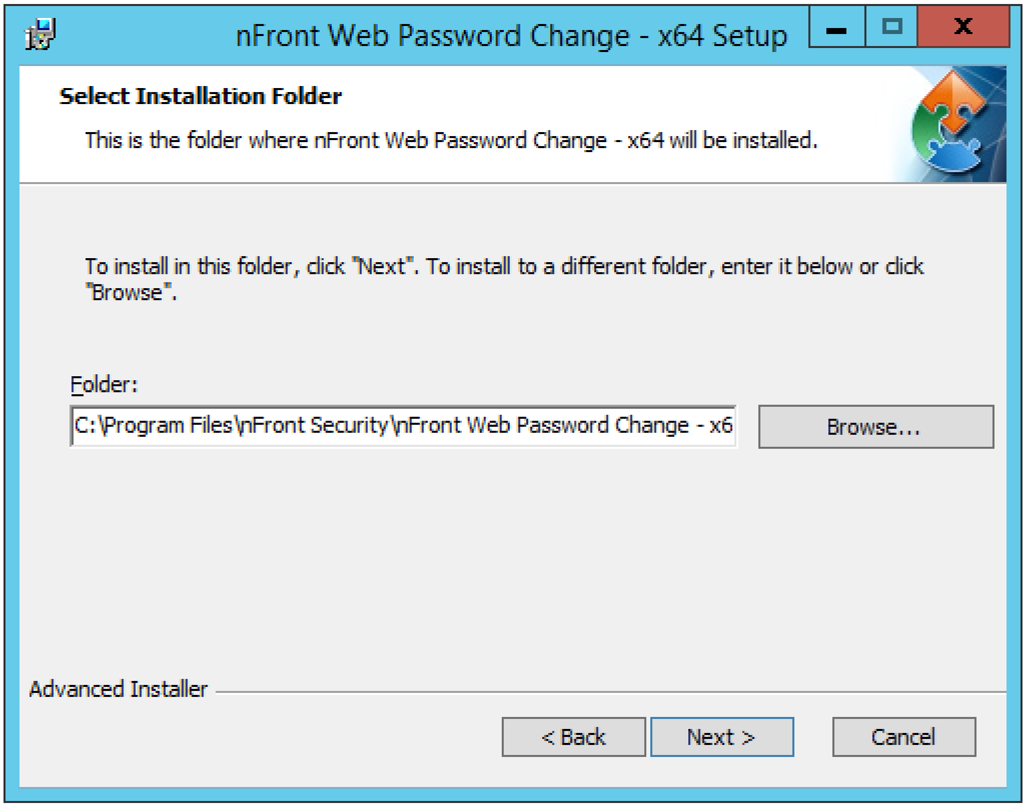
SOFTWARE LICENSE AGREEMENT

THIS SOFTWARE LICENSE AGREEMENT (the "Agreement") entered into by and between Altus Network Solutions, Inc., a Georgia corporation (the "Licensor"), and the undersigned customer (the "Licensee") determines the rights and licenses granted to the Licensee in the Licensed Software (hereinafter defined) supplied by the Licensor hereunder.

● I accept the terms in the License Agreement

○ I do not accept the terms in the License Agreement

Figure 2.2.6 –NPF-WEB Installer – Step 3



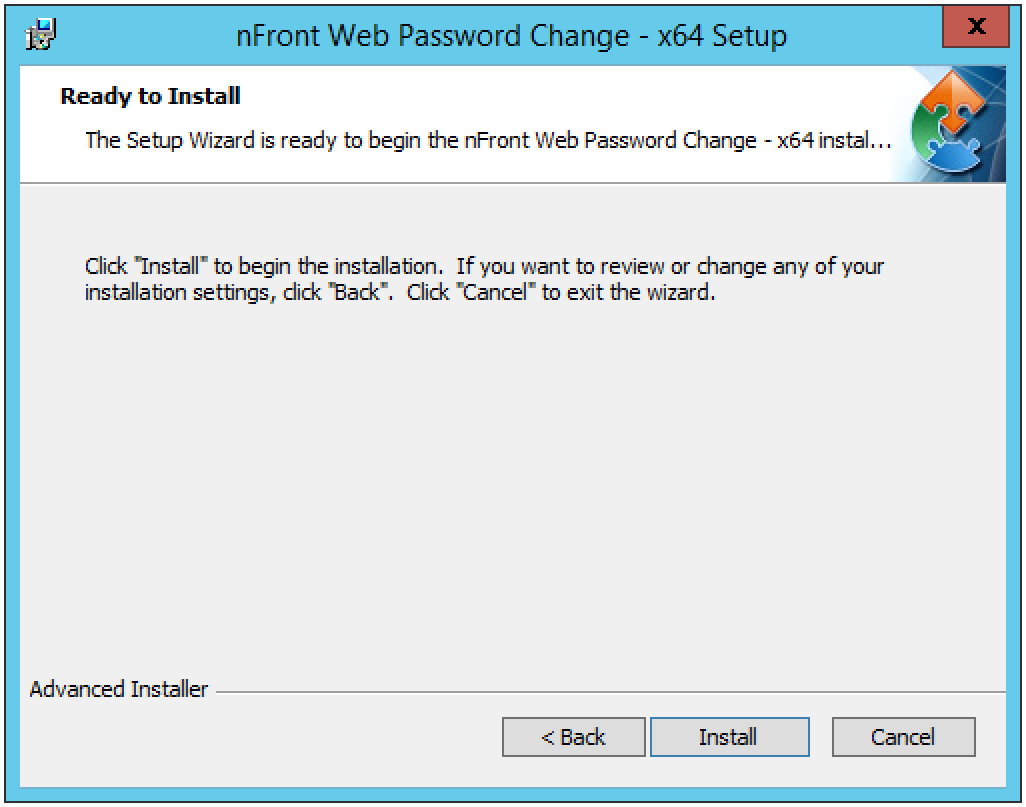
Select Installation Folder

This is the folder where nFront Web Password Change - x64 will be installed.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files\nFront Security\nFront Web Password Change - x6

Figure 2.2.7 –NPF-WEB Installer – Step 4

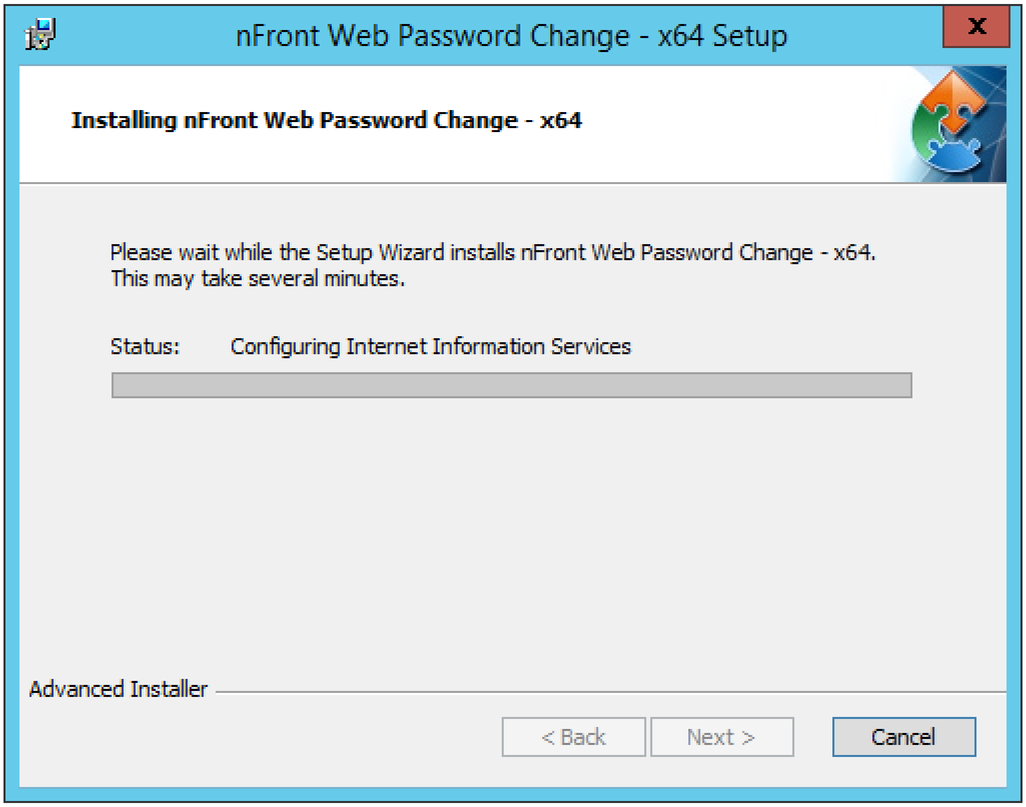


Ready to Install

The Setup Wizard is ready to begin the nFront Web Password Change - x64 instal...

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

Figure 2.2.8 –NPF-WEB Installer – Step 5

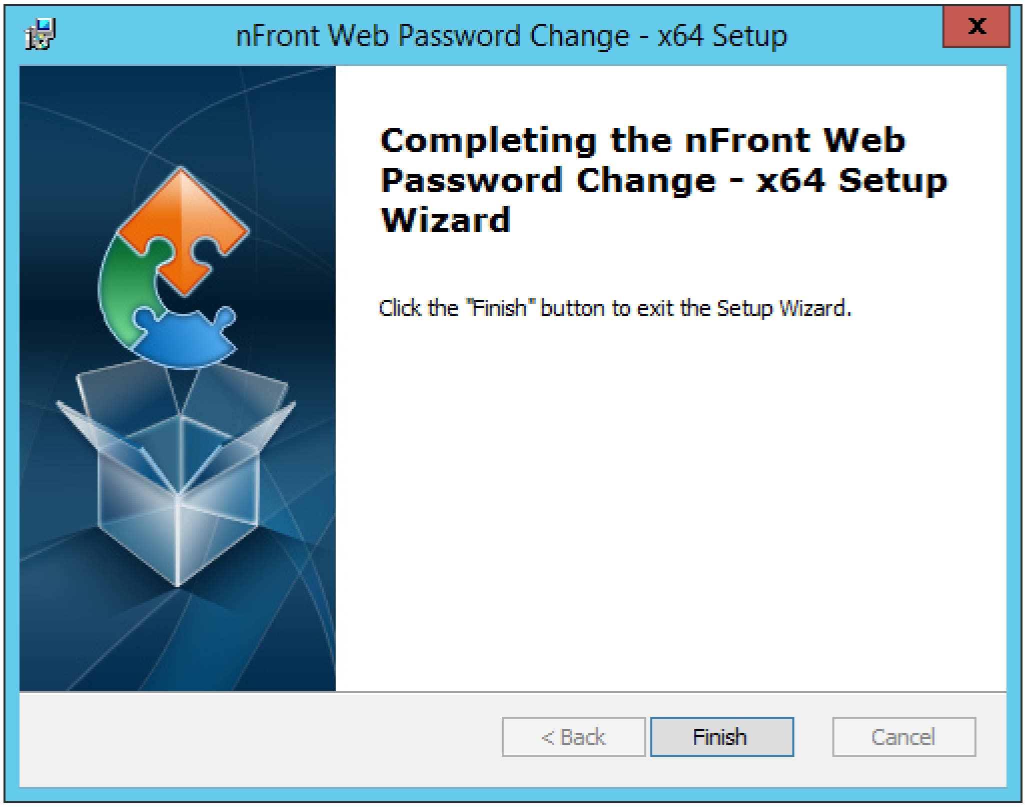


Installing nFront Web Password Change - x64

Please wait while the Setup Wizard installs nFront Web Password Change - x64.
This may take several minutes.

Status: Configuring Internet Information Services

Figure 2.2.9 –NPF-WEB Installer – Step 6



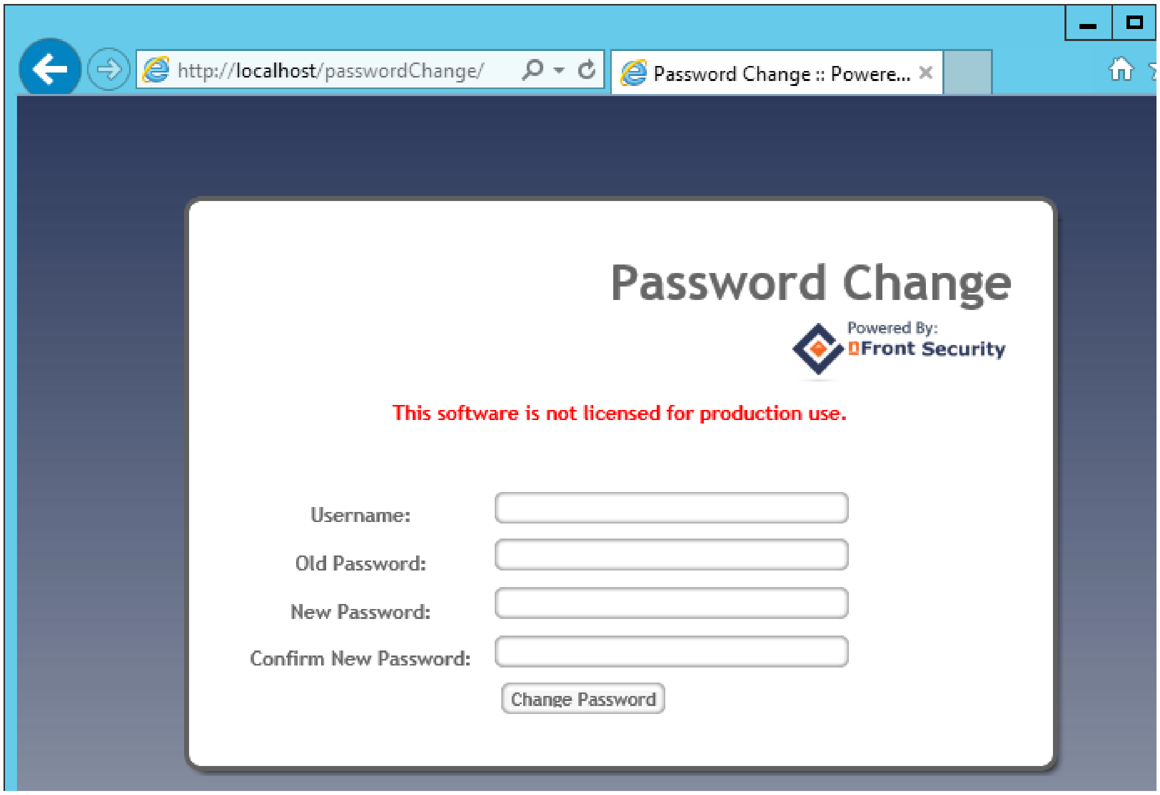
nFront Web Password Change - x64 Setup

Completing the nFront Web Password Change - x64 Setup Wizard

Click the "Finish" button to exit the Setup Wizard.

Figure 2.2.10 –NPF-WEB Installer – Step 7

Now a test of http://localhost/passwordChange should work as expected. After tying in a username and moving to another field the rules should populate with your nFront requirements.



http://localhost/passwordChange/
Password Change :: Powere...

Password Change

Powered By:
nFront Security

This software is not licensed for production use.

Username:

Old Password:

New Password:

Confirm New Password:

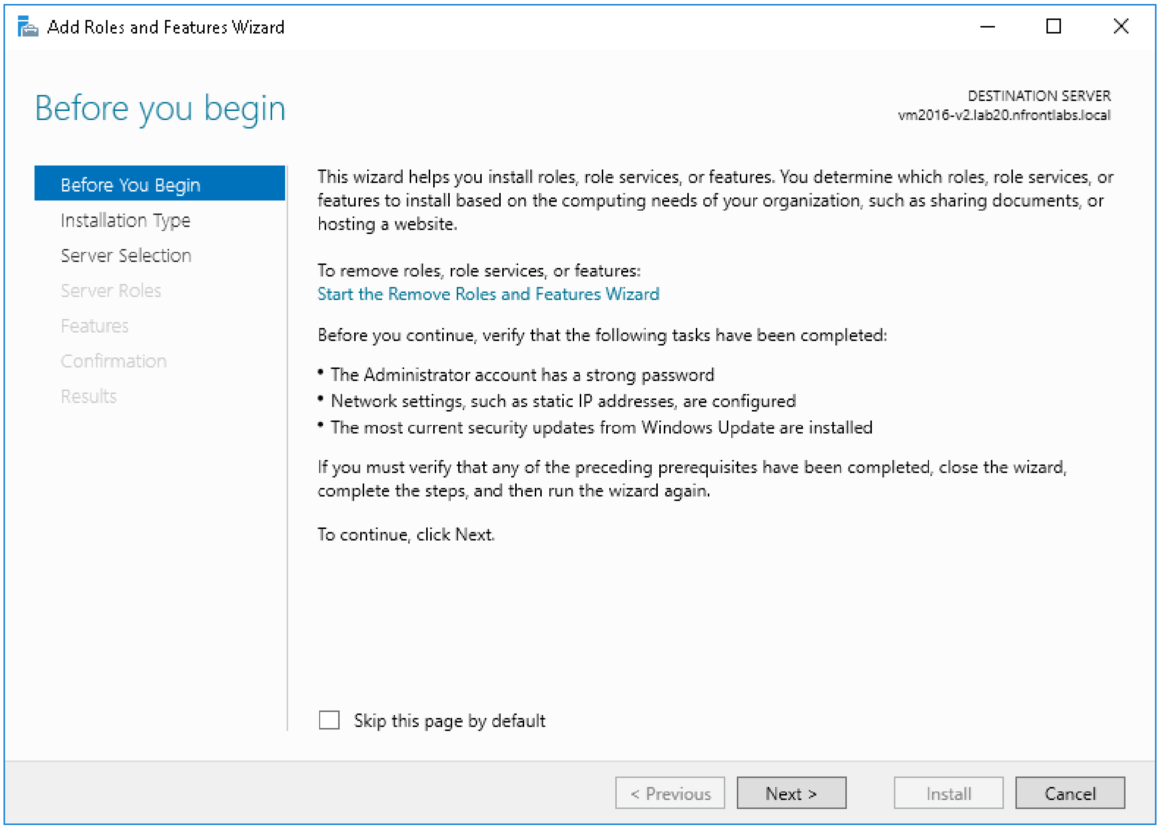
Figure 2.2.11 –NPF-WEB working on Server 2012 R2

2.3 Installation on Windows Server 2016

For the IIS configuration it is important to have:

- Windows Authentication (under Security category)
- ASP.NET 4.6 (under Application Development category)
- IIS 6 Metabase Compatibility (under Management Tools category)

If you already have IIS installed you can go back and add those items. The sceenshots below go through adding the Web Server (IIS) Role to a server that does not have it.



This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

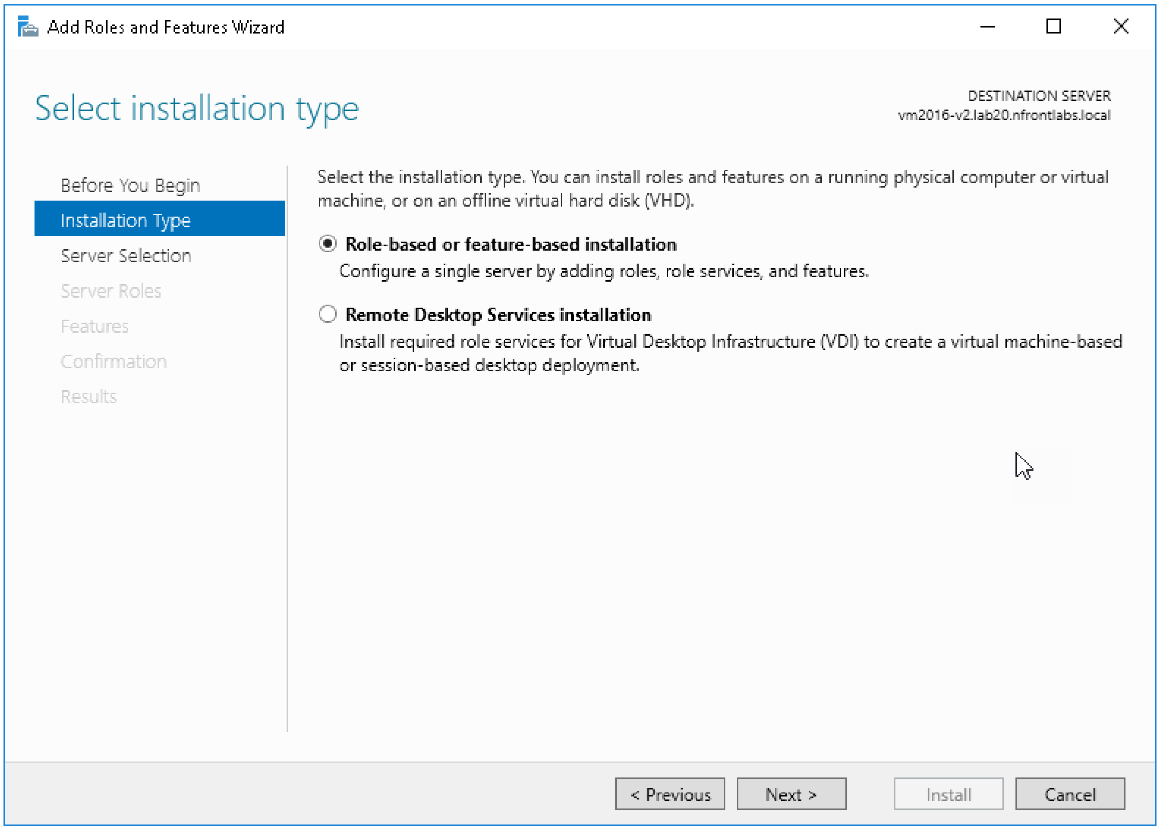
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

☐ Skip this page by default

Figure 2.3.1 – Server 2016 Add Roles Wizard Step 1



Select installation type

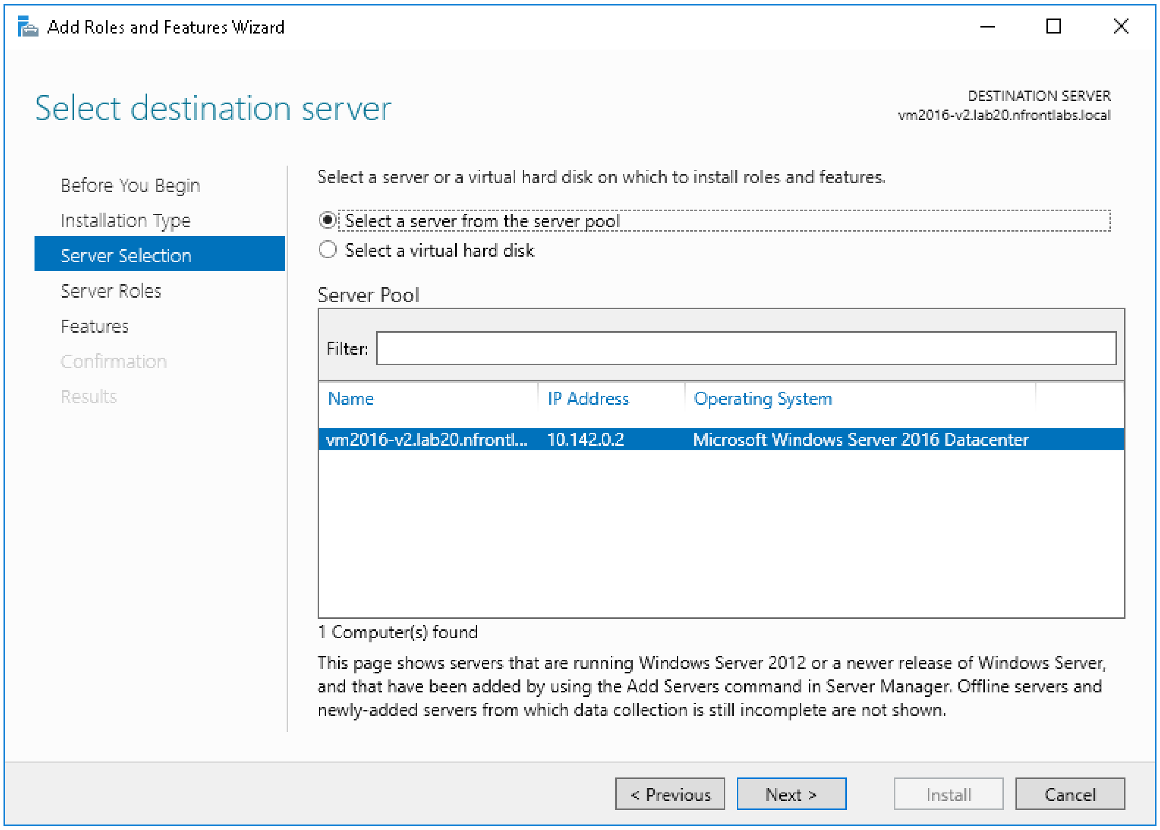
DESTINATION SERVER
vm2016-v2.lab20.nfrontlabs.local

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

Figure 2.3.2 – Server 2016 Add Roles Wizard Step 2



Select destination server

DESTINATION SERVER
vm2016-v2.lab20.nfrontlabs.local

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

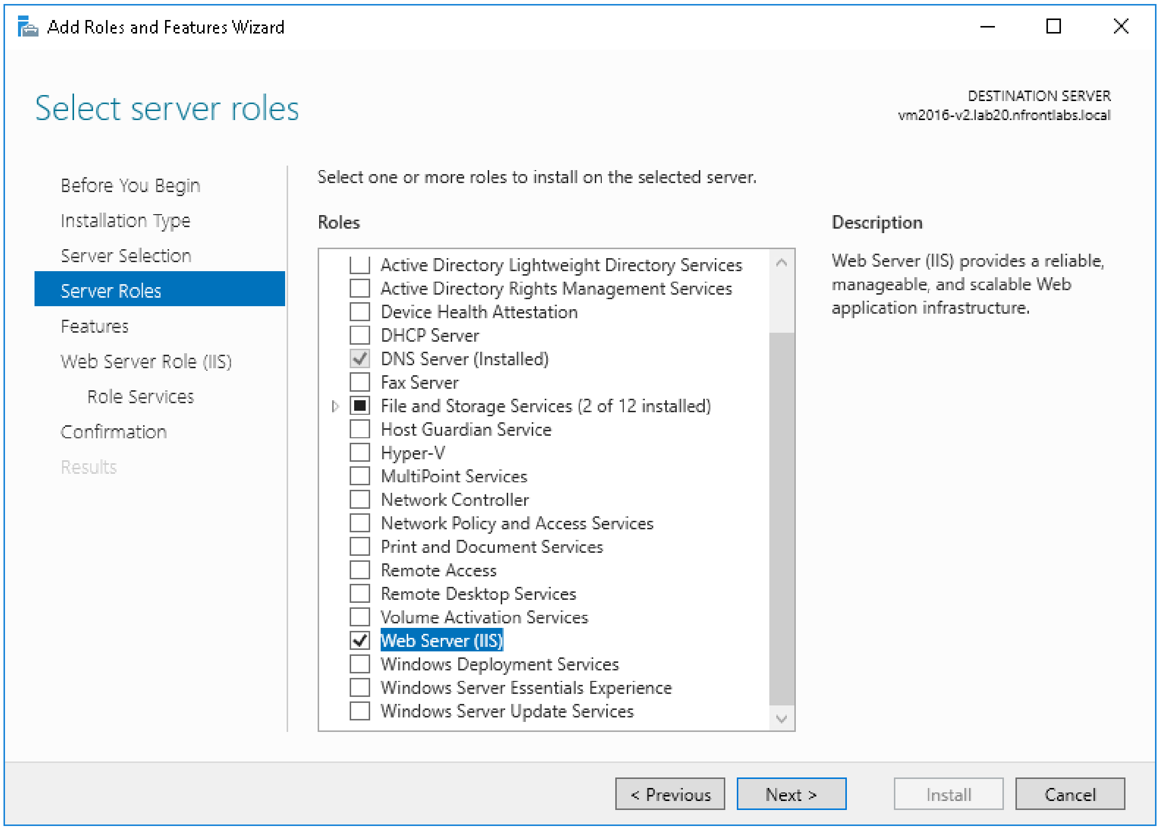
Filter:

Name	IP Address	Operating System
vm2016-v2.lab20.nfrontl...	10.142.0.2	Microsoft Windows Server 2016 Datacenter

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

Figure 2.3.3 – Server 2016 Add Roles Wizard Step 3



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
vm2016-v2.lab20.nfrontlabs.local

Select one or more roles to install on the selected server.

Roles

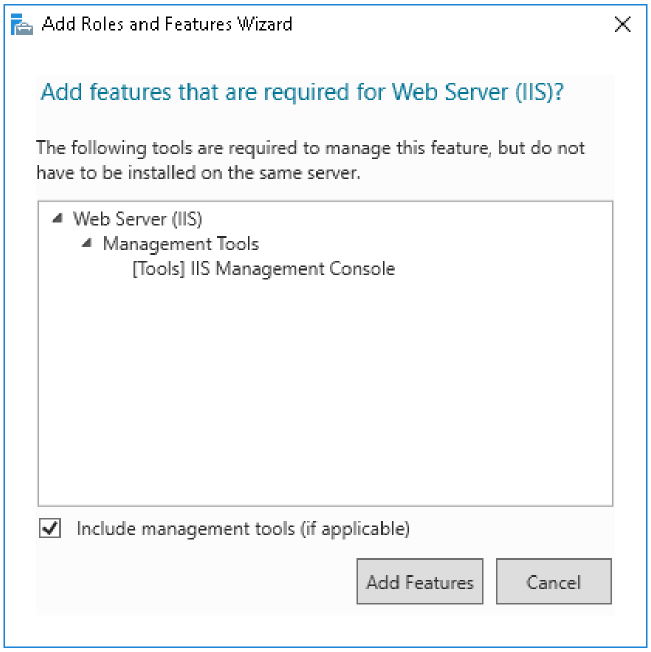
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- □ DHCP Server
- ☑ DNS Server (Installed)
- □ Fax Server
- ■ File and Storage Services (2 of 12 installed)
- □ Host Guardian Service
- □ Hyper-V
- □ MultiPoint Services
- □ Network Controller
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- ☑ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Essentials Experience
- □ Windows Server Update Services

Description

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

Figure 2.3.4 – Server 2016 Add Roles Wizard Step 4

When you select Web Server (IIS) you will be immediately prompted to add the Management tools. Click Add Features to continue.



Add Roles and Features Wizard

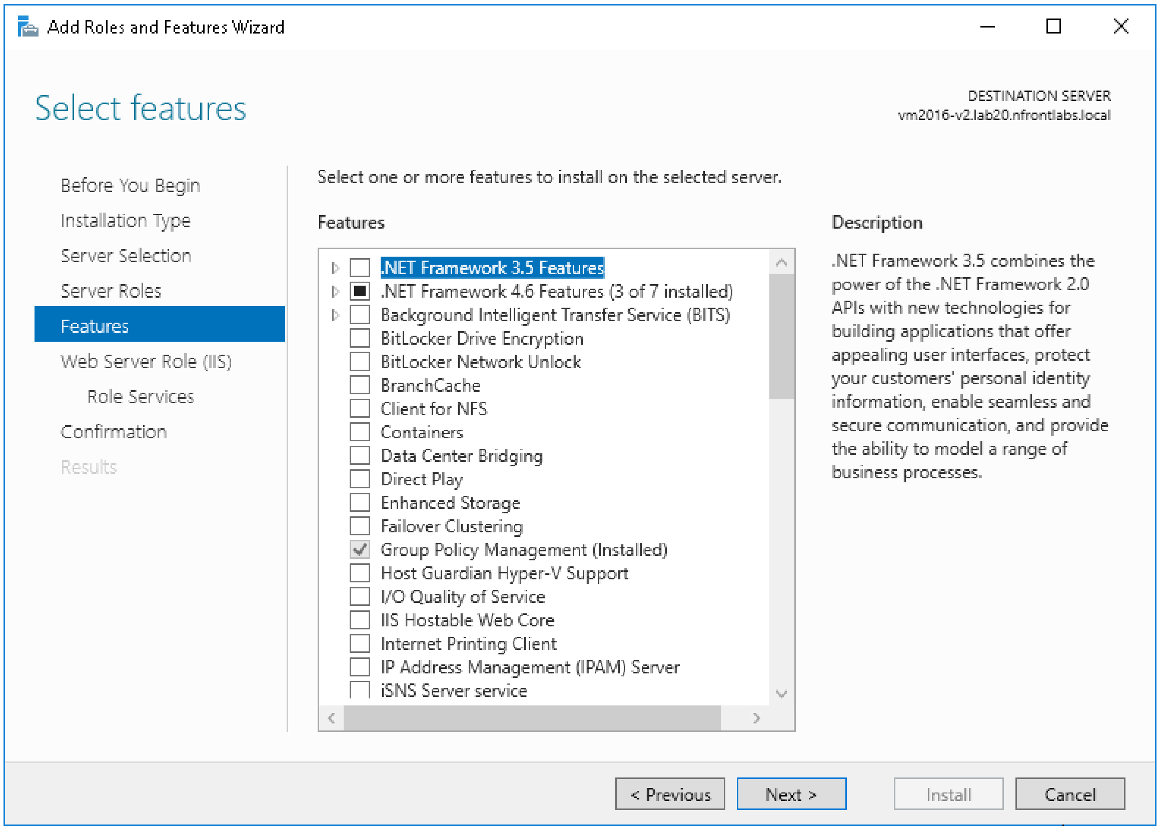
Add features that are required for Web Server (IIS)?

The following tools are required to manage this feature, but do not have to be installed on the same server.

- Web Server (IIS)
  - Management Tools
    - [Tools] IIS Management Console

☑ Include management tools (if applicable)

Figure 2.3.5 – Server 2016 Add Roles Wizard – adding management tools



Add Roles and Features Wizard

Select features

DESTINATION SERVER
vm2016-v2.lab20.nfrontlabs.local

Select one or more features to install on the selected server.

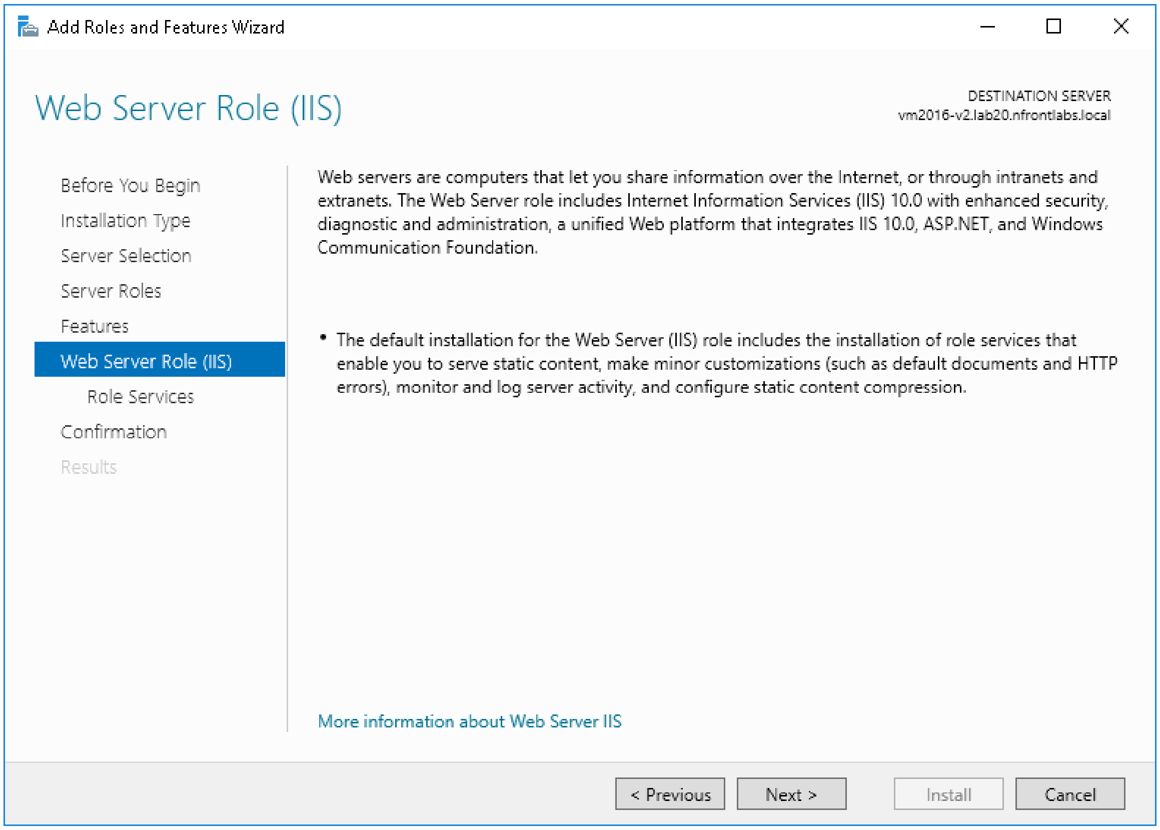
Features

- □ .NET Framework 3.5 Features
- ■ .NET Framework 4.6 Features (3 of 7 installed)
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BitLocker Network Unlock
- □ BranchCache
- □ Client for NFS
- □ Containers
- □ Data Center Bridging
- □ Direct Play
- □ Enhanced Storage
- □ Failover Clustering
- ☑ Group Policy Management (Installed)
- □ Host Guardian Hyper-V Support
- □ I/O Quality of Service
- □ IIS Hostable Web Core
- □ Internet Printing Client
- □ IP Address Management (IPAM) Server
- □ iSNS Server service

Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

Figure 2.3.6 – Server 2016 Add Roles Wizard Step 5



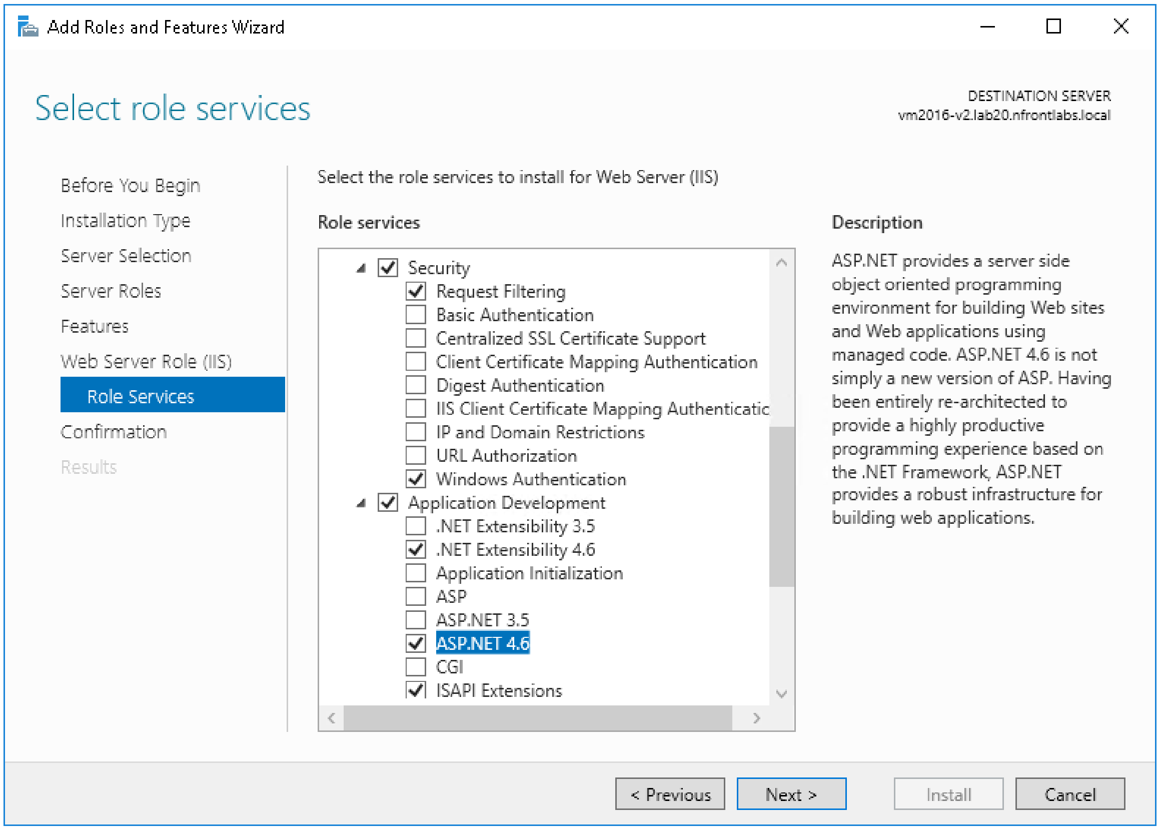
Web Server Role (IIS)

Web servers are computers that let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 10.0 with enhanced security, diagnostic and administration, a unified Web platform that integrates IIS 10.0, ASP.NET, and Windows Communication Foundation.

- The default installation for the Web Server (IIS) role includes the installation of role services that enable you to serve static content, make minor customizations (such as default documents and HTTP errors), monitor and log server activity, and configure static content compression.

More information about Web Server IIS

Figure 2.3.7 – Server 2016 Add Roles Wizard Step 6



Select role services

DESTINATION SERVER
vm2016-v2.lab20.nfrontlabs.local

Select the role services to install for Web Server (IIS)

Role services

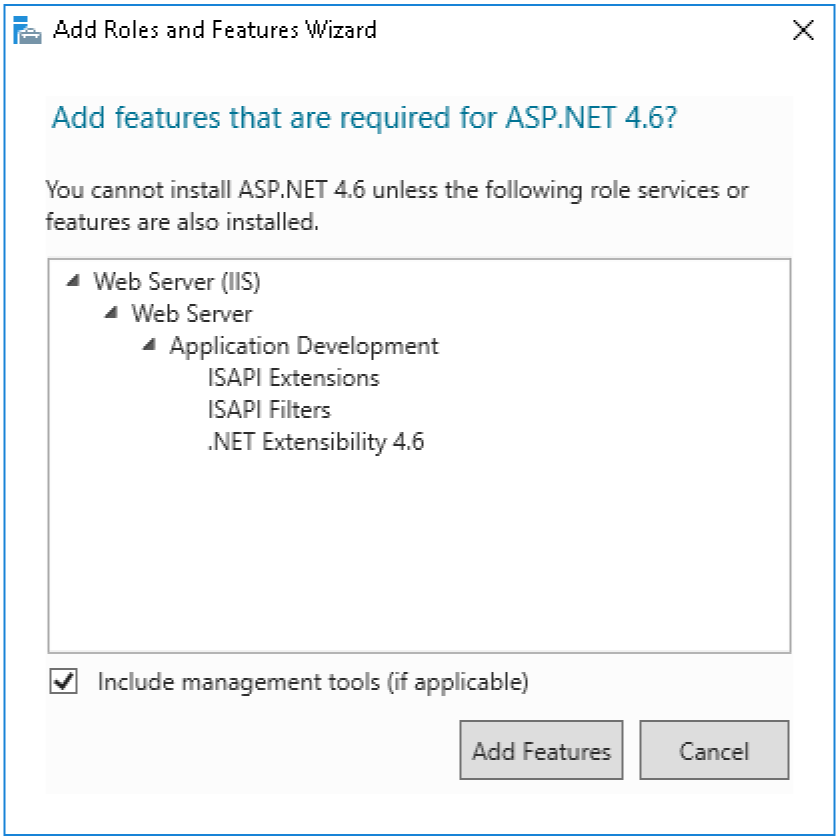
- ☑ Security
  - ☑ Request Filtering
  - ☐ Basic Authentication
  - ☐ Centralized SSL Certificate Support
  - ☐ Client Certificate Mapping Authentication
  - ☐ Digest Authentication
  - ☐ IIS Client Certificate Mapping Authenticatic
  - ☐ IP and Domain Restrictions
  - ☐ URL Authorization
  - ☑ Windows Authentication
- ☑ Application Development
  - ☐ .NET Extensibility 3.5
  - ☑ .NET Extensibility 4.6
  - ☐ Application Initialization
  - ☐ ASP
  - ☐ ASP.NET 3.5
  - ☑ ASP.NET 4.6
  - ☐ CGI
  - ☑ ISAPI Extensions

Description

ASP.NET provides a server side object oriented programming environment for building Web sites and Web applications using managed code. ASP.NET 4.6 is not simply a new version of ASP. Having been entirely re-architected to provide a highly productive programming experience based on the .NET Framework, ASP.NET provides a robust infrastructure for building web applications.

Figure 2.3.8 – Server 2016 Add Roles Wizard Step 7

When you select ASP.NET 4.6 you will be immediately prompted to add additional items. Click Add Features to continue.



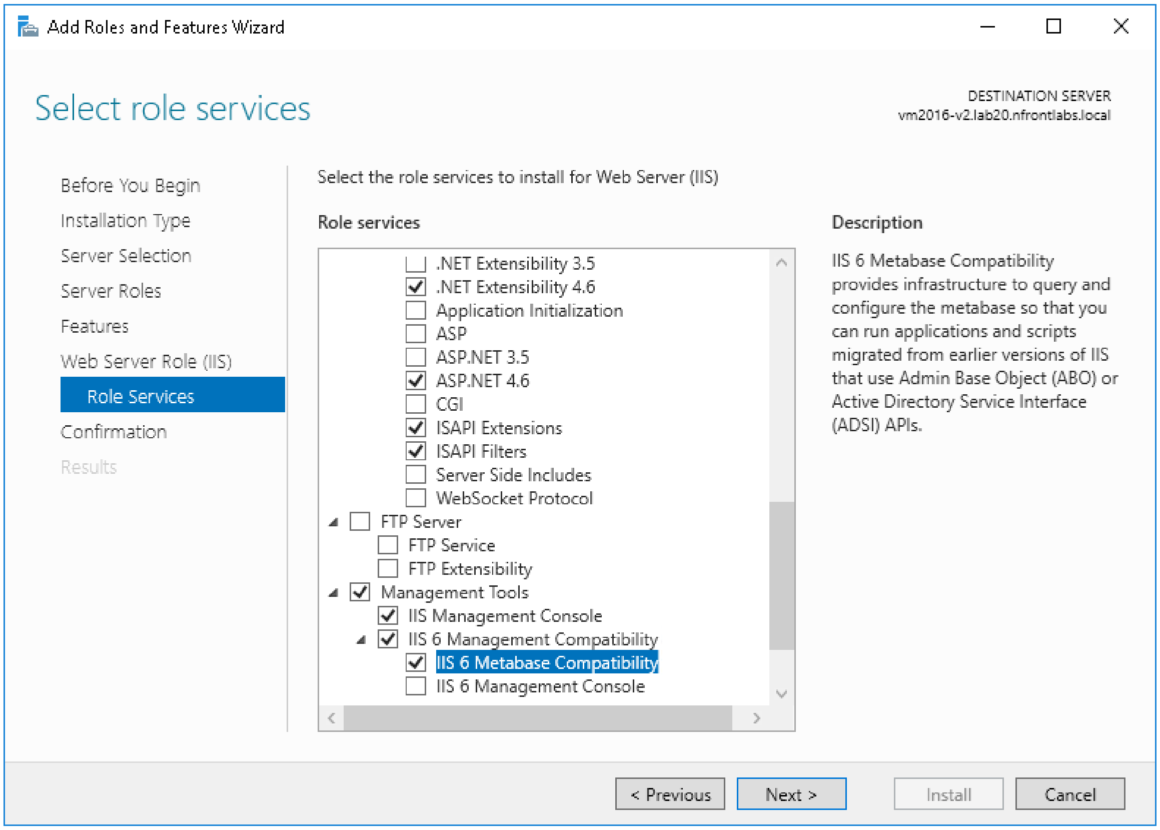
Add features that are required for ASP.NET 4.6?

You cannot install ASP.NET 4.6 unless the following role services or features are also installed.

- Web Server (IIS)
  - Web Server
    - Application Development
      - ISAPI Extensions
      - ISAPI Filters
      - .NET Extensibility 4.6

☑ Include management tools (if applicable)

Figure 2.3.9 – Server 2016 Add Roles Wizard – adding ASP.NET features



Add Roles and Features Wizard

Select role services

DESTINATION SERVER
vm2016-v2.lab20.nfrontlabs.local

Select the role services to install for Web Server (IIS)

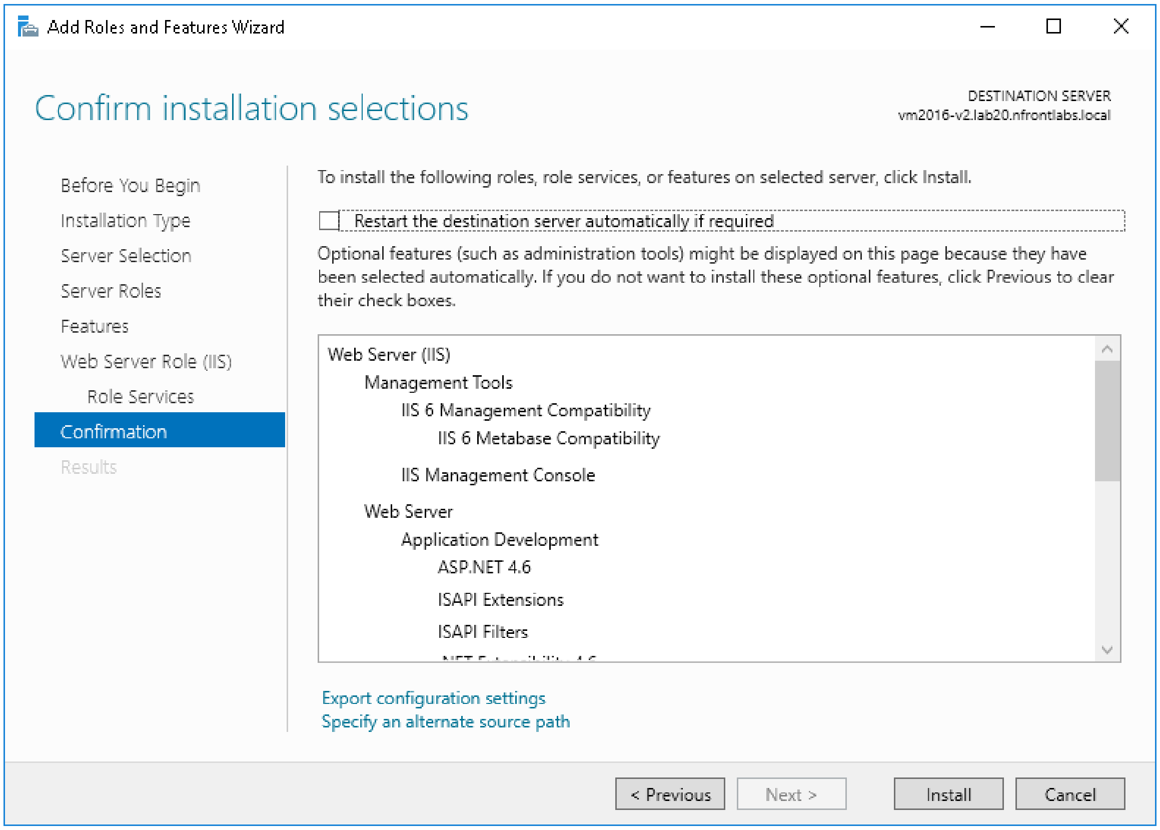
Role services

- □ .NET Extensibility 3.5
- ☑ .NET Extensibility 4.6
- □ Application Initialization
- □ ASP
- □ ASP.NET 3.5
- ☑ ASP.NET 4.6
- □ CGI
- ☑ ISAPI Extensions
- ☑ ISAPI Filters
- □ Server Side Includes
- □ WebSocket Protocol
- □ FTP Server
  - □ FTP Service
  - □ FTP Extensibility
- ☑ Management Tools
  - ☑ IIS Management Console
  - ☑ IIS 6 Management Compatibility
    - ☑ IIS 6 Metabase Compatibility
    - □ IIS 6 Management Console

Description

IIS 6 Metabase Compatibility provides infrastructure to query and configure the metabase so that you can run applications and scripts migrated from earlier versions of IIS that use Admin Base Object (ABO) or Active Directory Service Interface (ADSI) APIs.

Figure 2.3.10 – Server 2016 Add Roles Wizard Step 8



Confirm installation selections

DESTINATION SERVER
vm2016-v2.lab20.nfrontlabs.local

To install the following roles, role services, or features on selected server, click Install.

□ Restart the destination server automatically if required

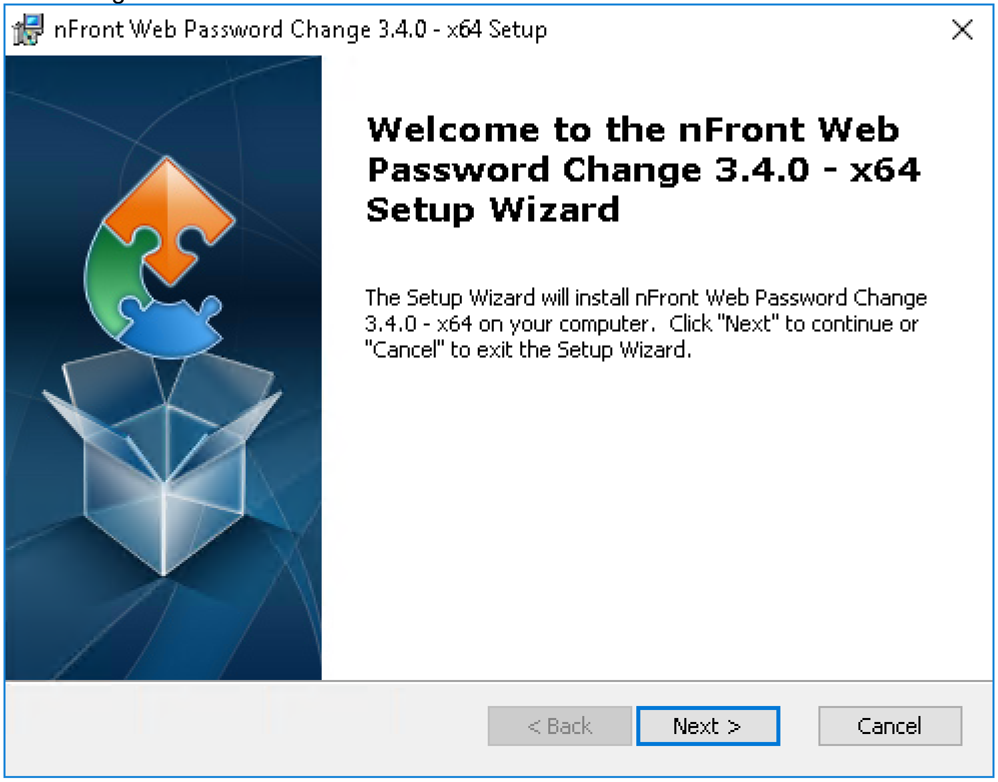
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

```
Web Server (IIS)
    Management Tools
        IIS 6 Management Compatibility
            IIS 6 Metabase Compatibility

        IIS Management Console

    Web Server
        Application Development
            ASP.NET 4.6

            ISAPI Extensions

            ISAPI Filters
```

Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel

Figure 2.3.11 – Server 2016 Add Roles Wizard Step 9

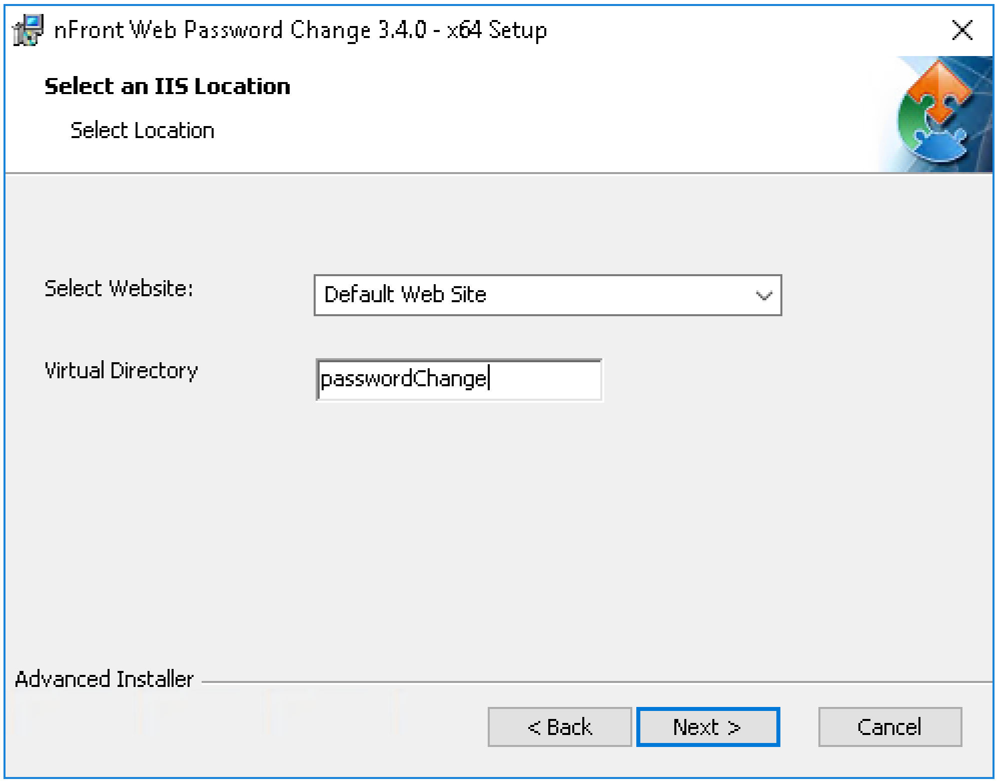
After the IIS Role is successfully added you can proceed with the installation of nFront Web Password Change.



Welcome to the nFront Web Password Change 3.4.0 - x64 Setup Wizard

The Setup Wizard will install nFront Web Password Change 3.4.0 - x64 on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

Figure 2.3.12 –NPF-WEB Installer – Step 1



nFront Web Password Change 3.4.0 - x64 Setup

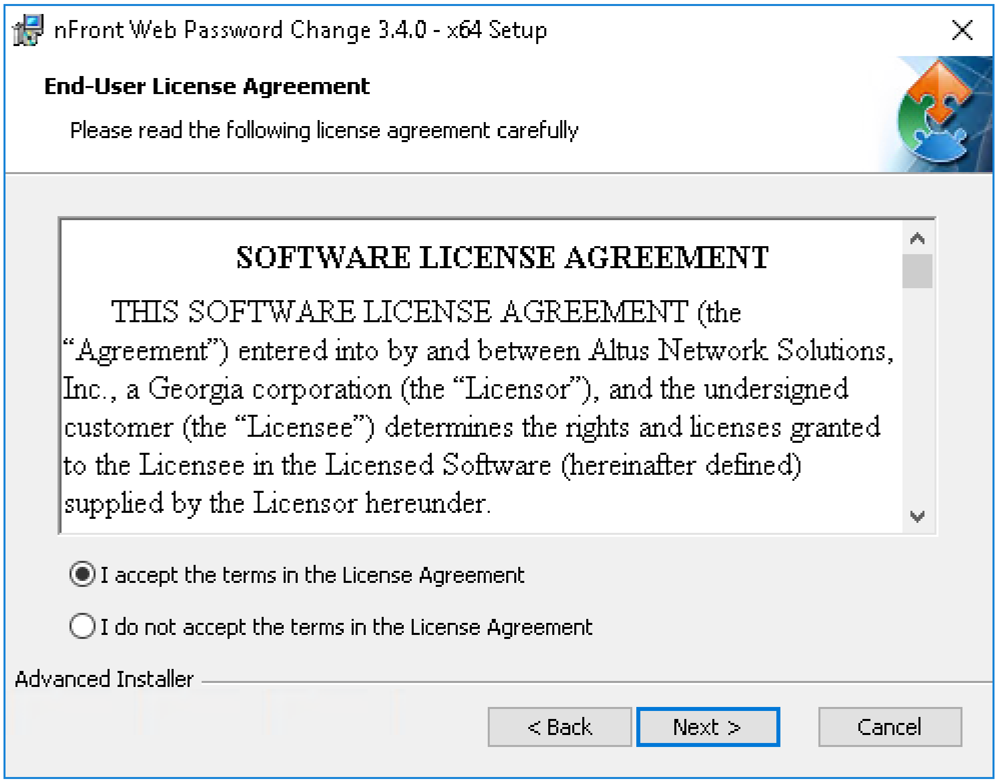
Select an IIS Location

Select Location

Select Website: Default Web Site

Virtual Directory: passwordChange

Figure 2.3.13 –NPF-WEB Installer – Step 2



nFront Web Password Change 3.4.0 - x64 Setup

End-User License Agreement

Please read the following license agreement carefully

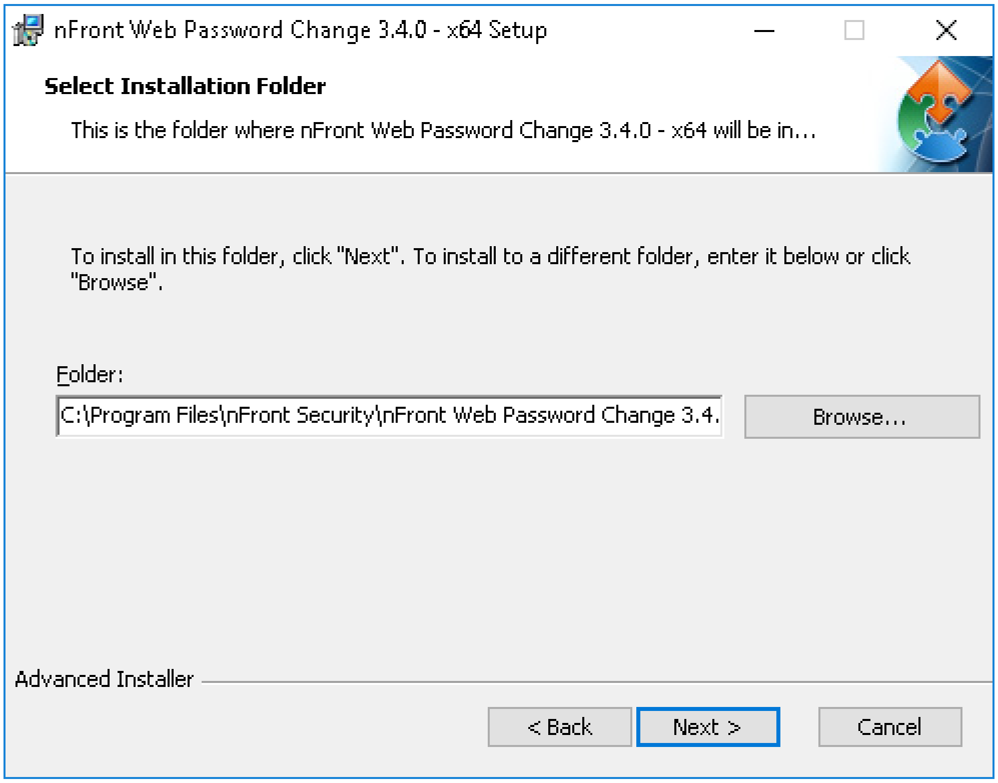
SOFTWARE LICENSE AGREEMENT

THIS SOFTWARE LICENSE AGREEMENT (the "Agreement") entered into by and between Altus Network Solutions, Inc., a Georgia corporation (the "Licensor"), and the undersigned customer (the "Licensee") determines the rights and licenses granted to the Licensee in the Licensed Software (hereinafter defined) supplied by the Licensor hereunder.

● I accept the terms in the License Agreement

○ I do not accept the terms in the License Agreement

Figure 2.3.14 –NPF-WEB Installer – Step 3



nFront Web Password Change 3.4.0 - x64 Setup

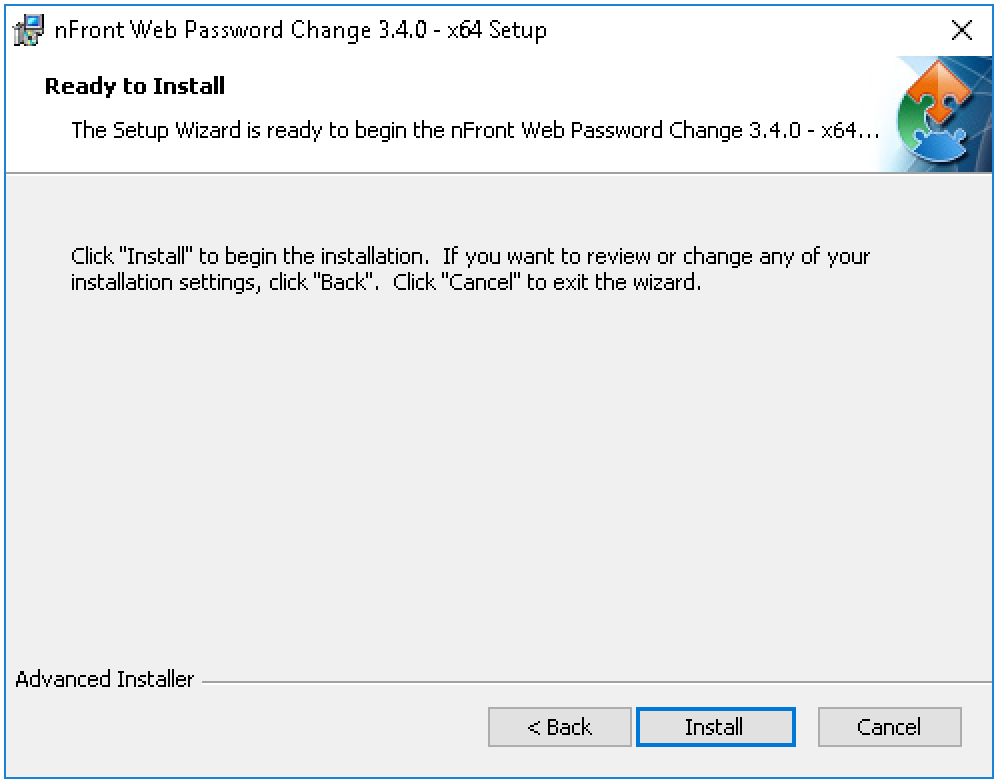
Select Installation Folder

This is the folder where nFront Web Password Change 3.4.0 - x64 will be in...

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files\nFront Security\nFront Web Password Change 3.4.

Figure 2.3.15 –NPF-WEB Installer – Step 4

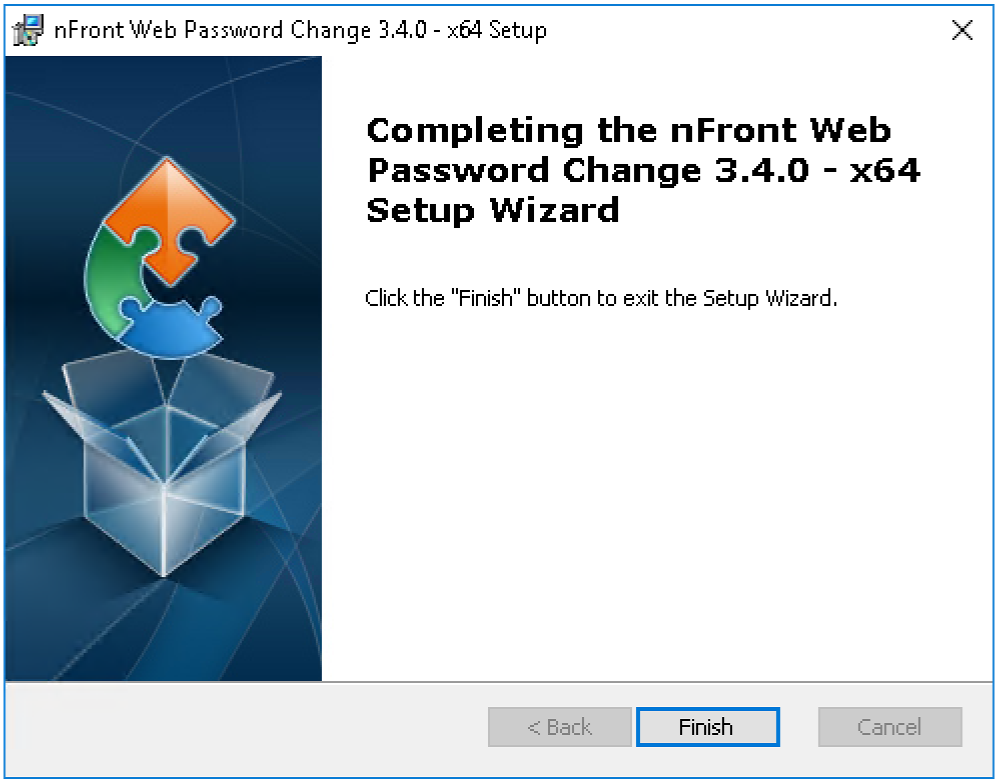


Ready to Install

The Setup Wizard is ready to begin the nFront Web Password Change 3.4.0 - x64...

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

Figure 2.3.16 –NPF-WEB Installer – Step 5



Completing the nFront Web Password Change 3.4.0 - x64 Setup Wizard

Click the "Finish" button to exit the Setup Wizard.

Figure 2.3.17 –NPF-WEB Installer – Step 6

2.4 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 2.4.1.

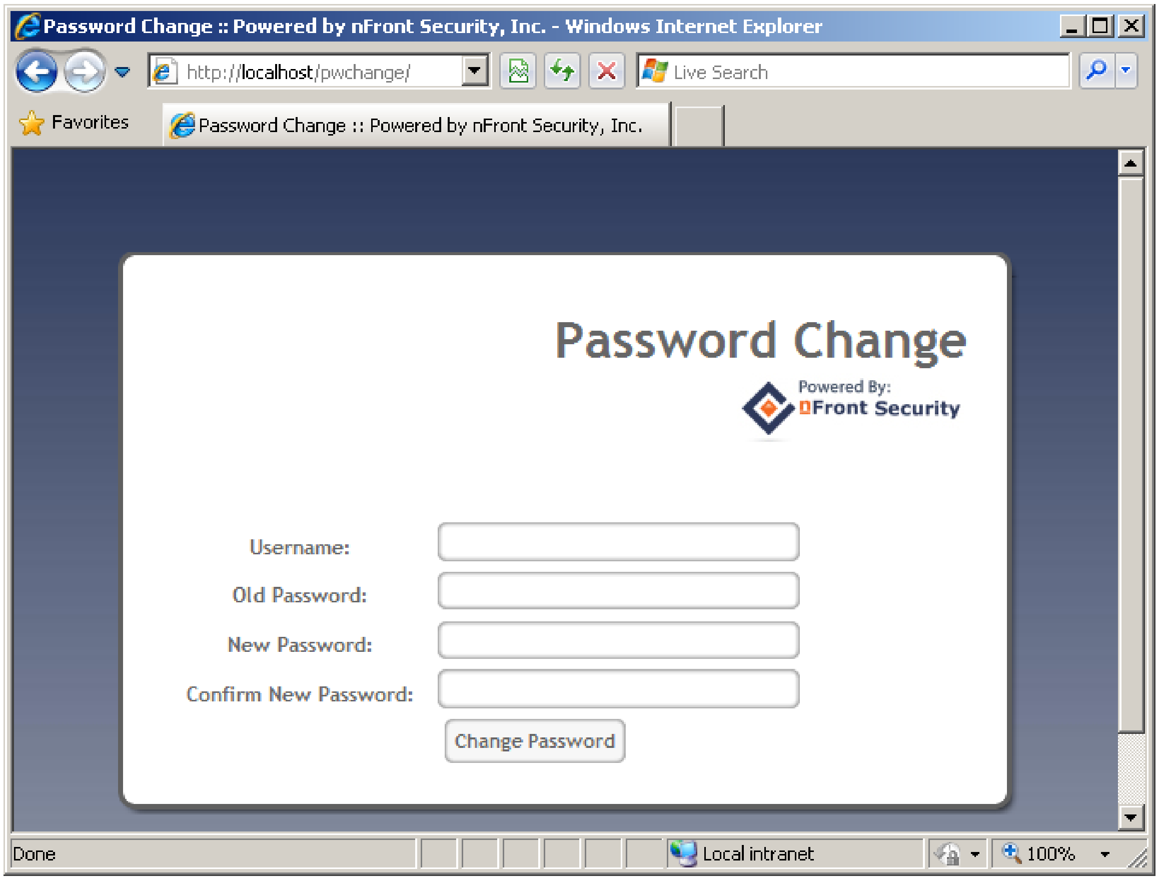
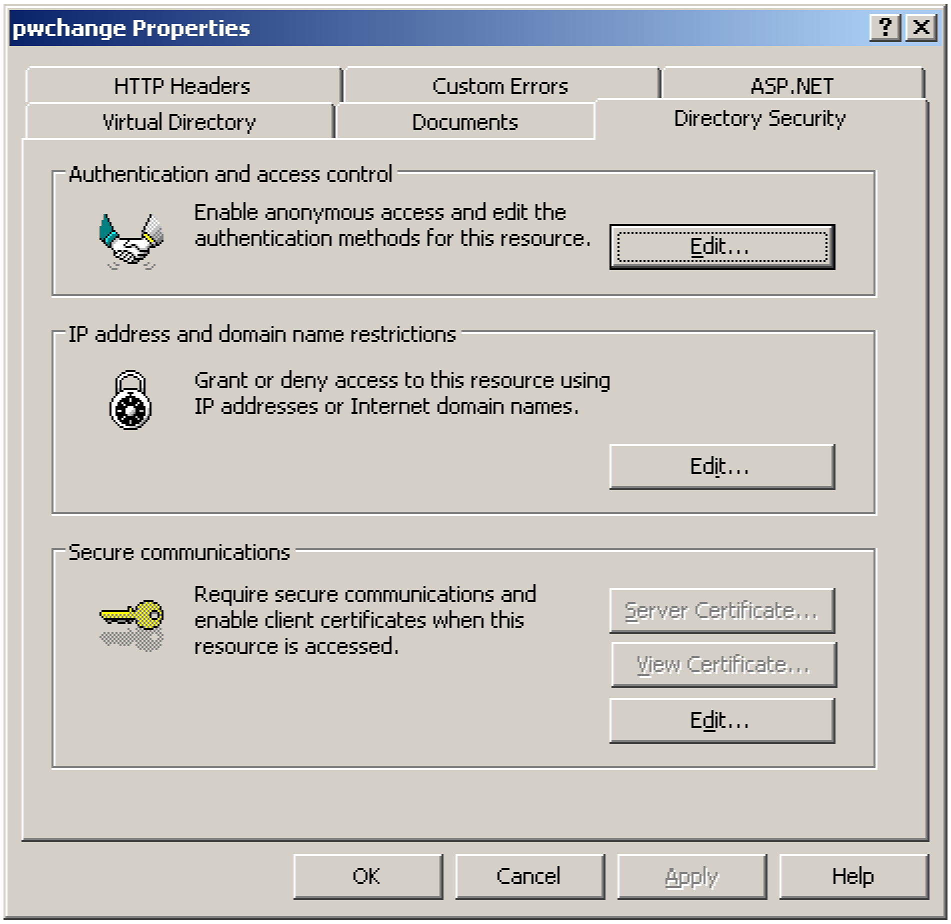

Password Change :: Powered by nFront Security, Inc. - Windows Internet Explorer
http://localhost/pwchange/
Live Search
Favorites
Password Change :: Powered by nFront Security, Inc.
Password Change
Powered By:
nFront Security
Username:
Old Password:
New Password:
Confirm New Password:
Change Password
Done
Local intranet
100%

Figure 2.4.1: 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 2.4.2). 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 2.4.3).



Authentication and access control

Enable anonymous access and edit the authentication methods for this resource.

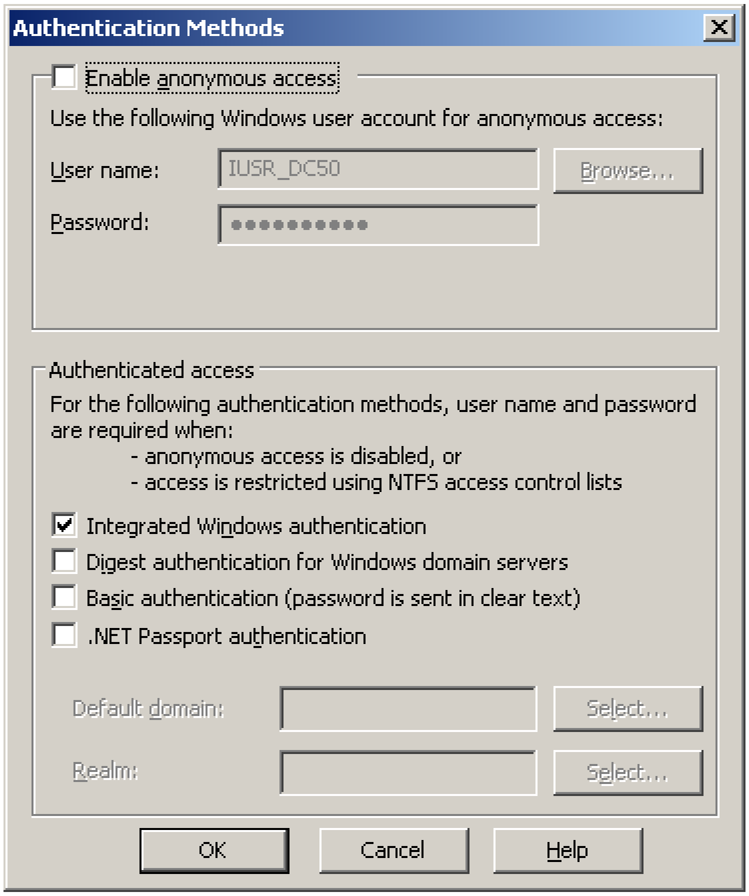
IP address and domain name restrictions

Grant or deny access to this resource using IP addresses or Internet domain names.

Secure communications

Require secure communications and enable client certificates when this resource is accessed.

Figure 2.4.2: Properties of virtual directory for application



Authentication Methods

□ Enable anonymous access

Use the following Windows user account for anonymous access:

User name: IUSR_DC50

Password: ●●●●●●●●●●

Authenticated access

For the following authentication methods, user name and password are required when:

- anonymous access is disabled, or
- access is restricted using NTFS access control lists

☑ Integrated Windows authentication

□ Digest authentication for Windows domain servers

□ Basic authentication (password is sent in clear text)

□ .NET Passport authentication

Default domain:

Realm:

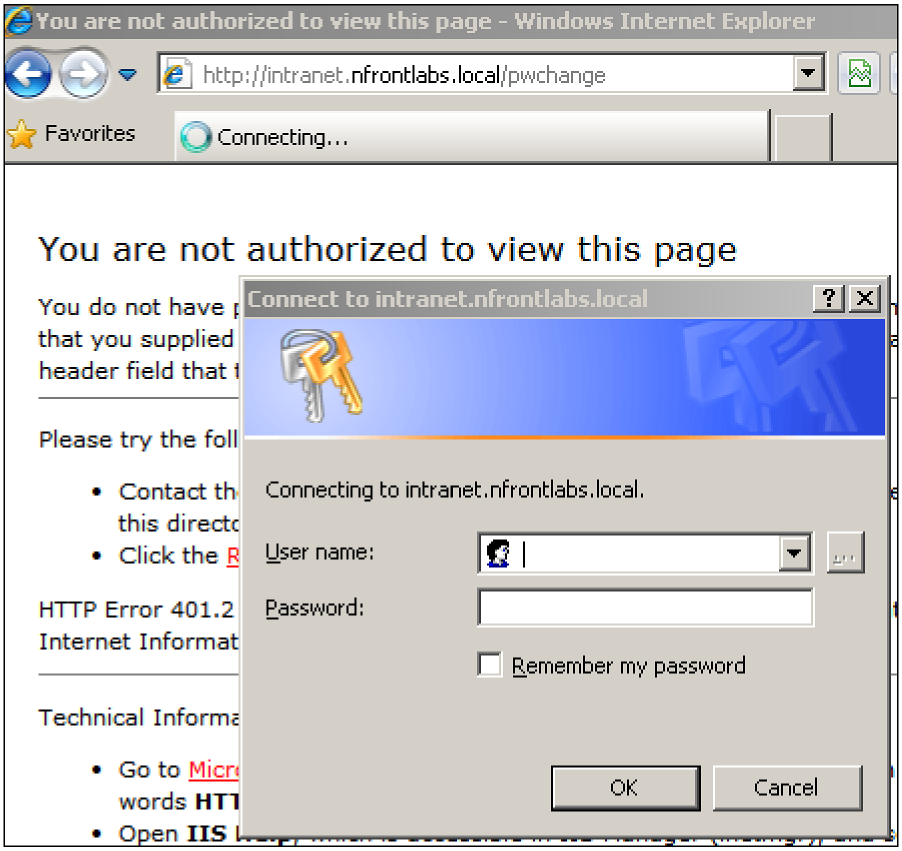
Figure 2.4.3: Authentication Methods for web application virtual directory

2.5 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 2.5.1).

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/.



You are not authorized to view this page - Windows Internet Explorer

http://intranet.nfrontlabs.local/pwchange

Connecting...

You are not authorized to view this page

Connect to intranet.nfrontlabs.local

Connecting to intranet.nfrontlabs.local.

User name:

Password:

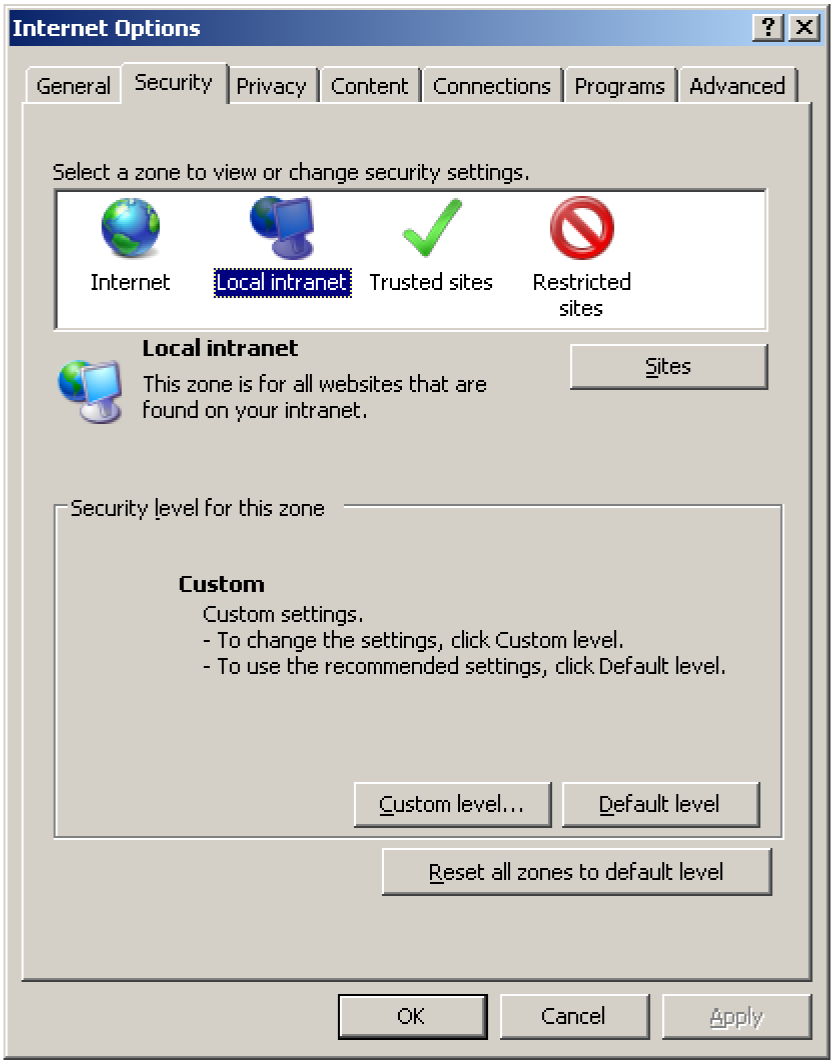
□ Remember my password

Figure 2.5.1: 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.

2.5.1 Manually modifying Local Intranet settings in Internet Explorer

In Internet Explorer go to Tools + Internet Options + Security Tab (Figure 2.5.1A)



Select a zone to view or change security settings.

Local intranet

This zone is for all websites that are found on your intranet.

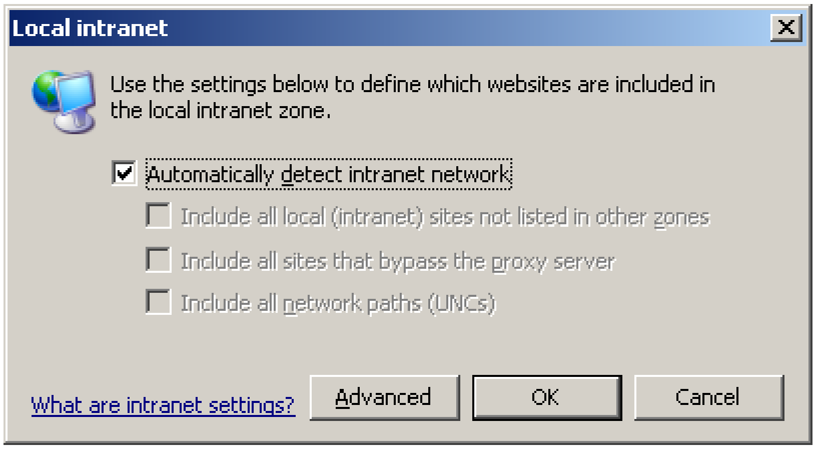
Security level for this zone

Custom

Custom settings.
- To change the settings, click Custom level.
- To use the recommended settings, click Default level.

Figure 2.5.1A: 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 2.5.1B).



Use the settings below to define which websites are included in the local intranet zone.

☑ Automatically detect intranet network

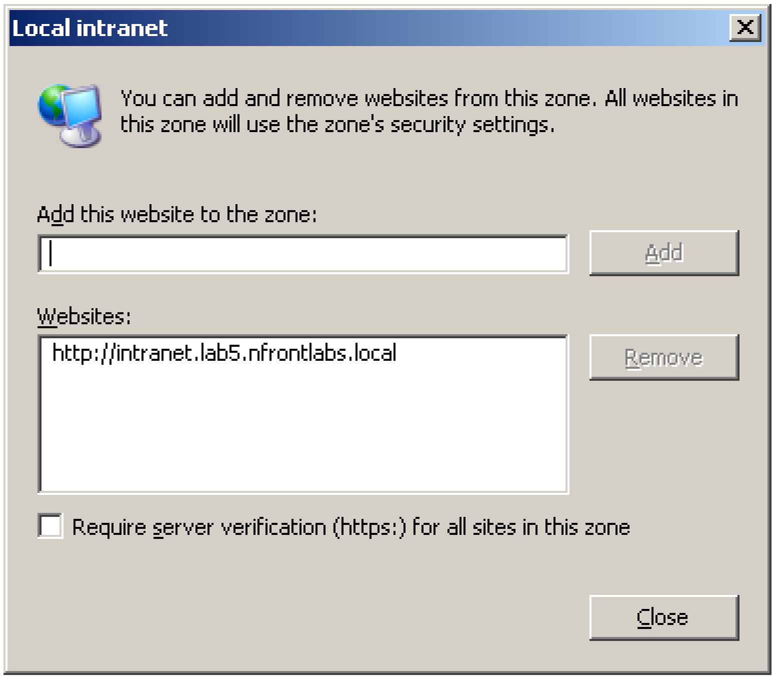
□ Include all local (intranet) sites not listed in other zones

□ Include all sites that bypass the proxy server

□ Include all network paths (UNCs)

Figure 2.5.1B: IE Local intranet zone settings

Click on the Advanced button to add your website to the zone (Figure 2.5.1C). 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.



You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:

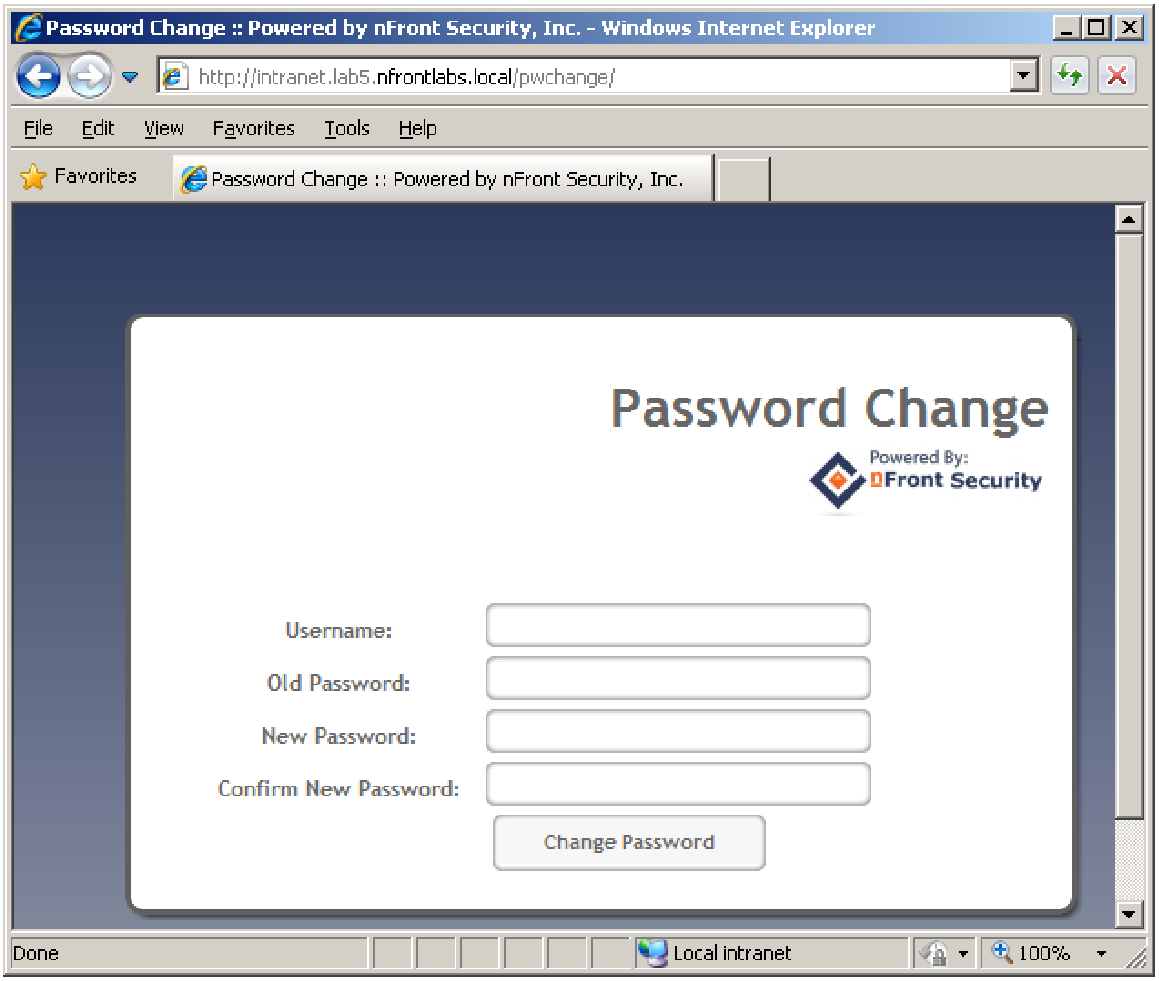
Websites:

http://intranet.lab5.nfrontlabs.local

□ Require server verification (https:) for all sites in this zone

Figure 2.5.1C: 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.


Password Change :: Powered by nFront Security, Inc. - Windows Internet Explorer
http://intranet.lab5.nfrontlabs.local/pwchange/
File
Edit
View
Favorites
Tools
Help
Favorites
Password Change :: Powered by nFront Security, Inc.
Password Change
Powered By:
nFront Security
Username:
Old Password:
New Password:
Confirm New Password:
Change Password
Done
Local intranet
100%

2.6 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.

2.7 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

*All REG_DWORD settings are 32-bit values

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\nFront Security\Web Password Change\altUID, REG_DWORD	Modifies the interface to provide rules and failure message in the locale specified by altUID. Locales supported: 1031 – German 1036 – French 1040 – Italian 3082 - Spanish
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.

2.8 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.

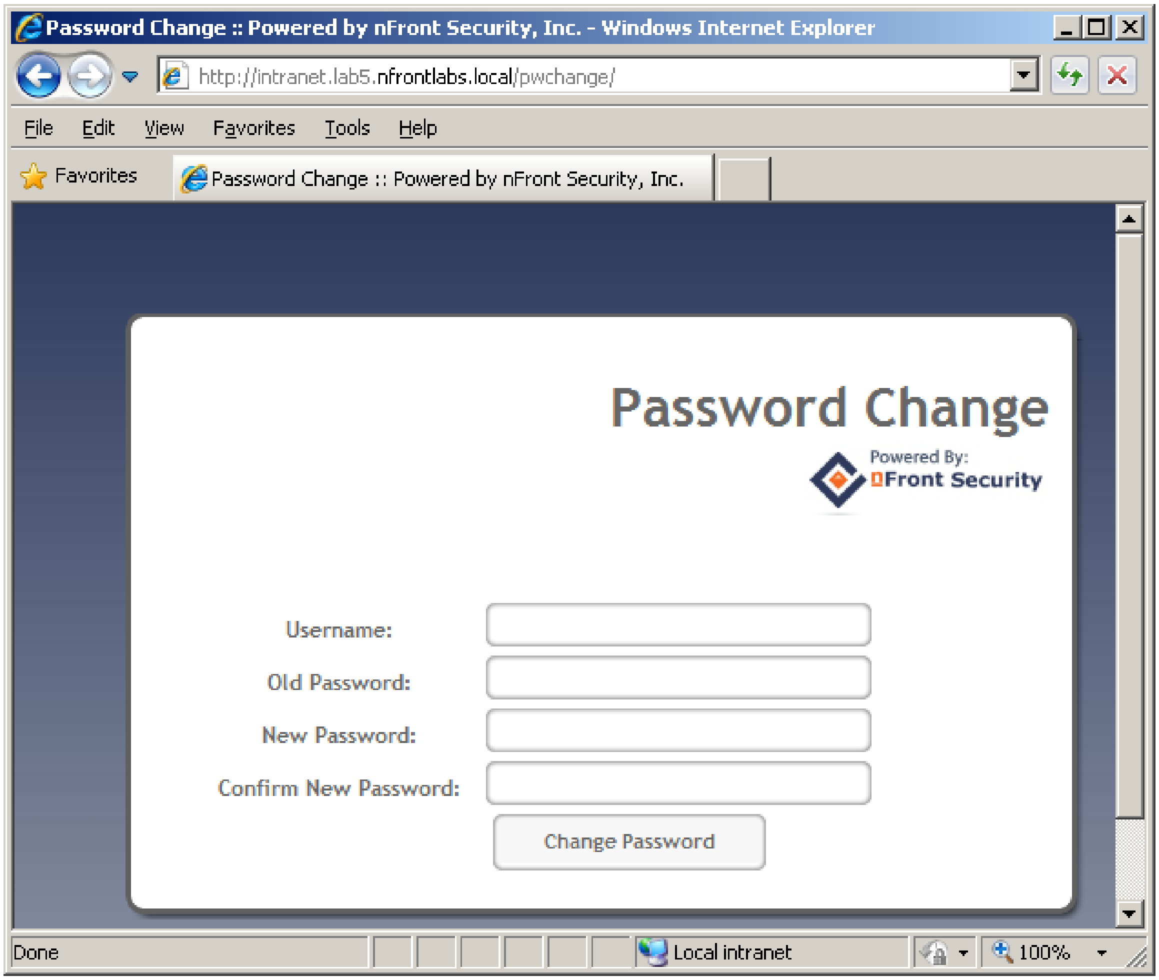
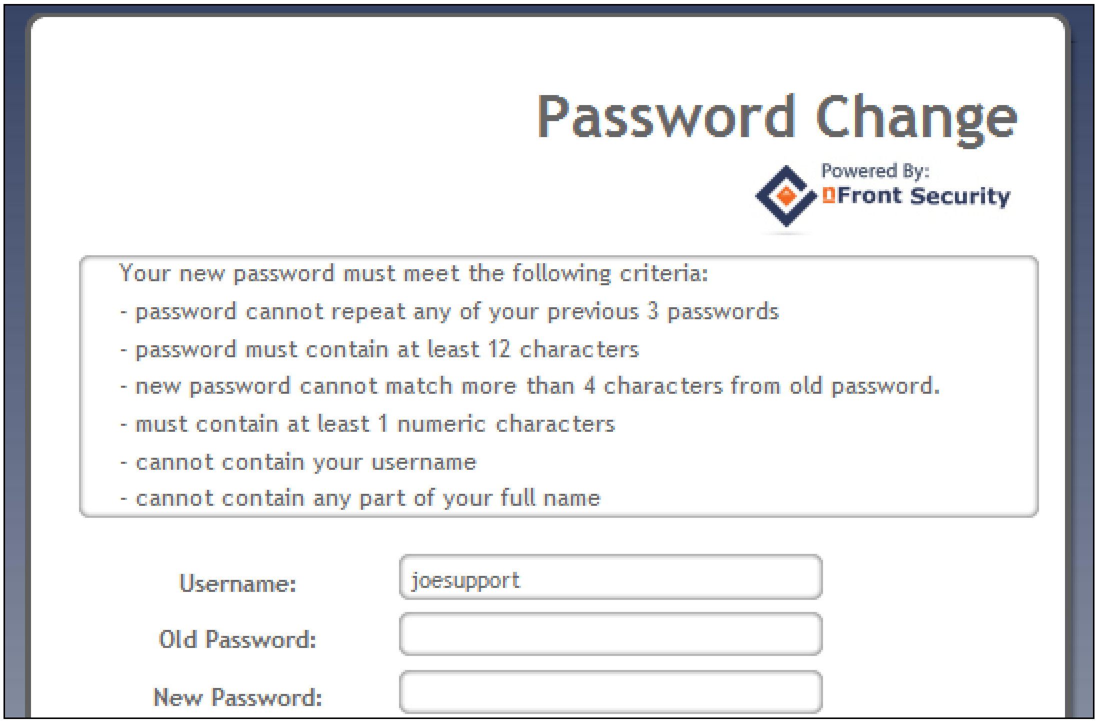

Password Change :: Powered by nFront Security, Inc. - Windows Internet Explorer
http://intranet.lab5.nfrontlabs.local/pwchange/
File
Edit
View
Favorites
Tools
Help
Favorites
Password Change :: Powered by nFront Security, Inc.
Password Change
Powered By:
nFront Security
Username:
Old Password:
New Password:
Confirm New Password:
Change Password
Done
Local intranet
100%

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.



Your new password must meet the following criteria:
- password cannot repeat any of your previous 3 passwords
- password must contain at least 12 characters
- new password cannot match more than 4 characters from old password.
- must contain at least 1 numeric characters
- cannot contain your username
- cannot contain any part of your full name

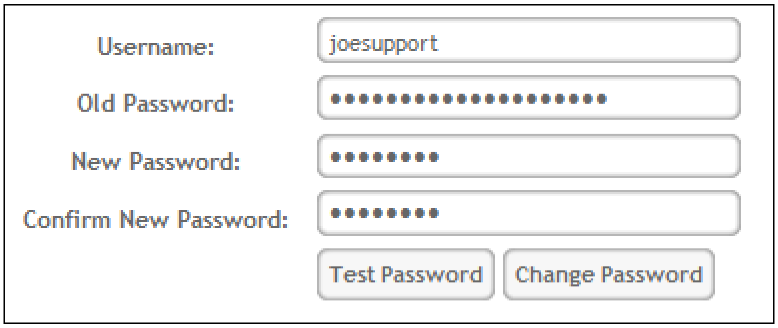
Username: joesupport

Old Password:

New Password:

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).



Username: joesupport

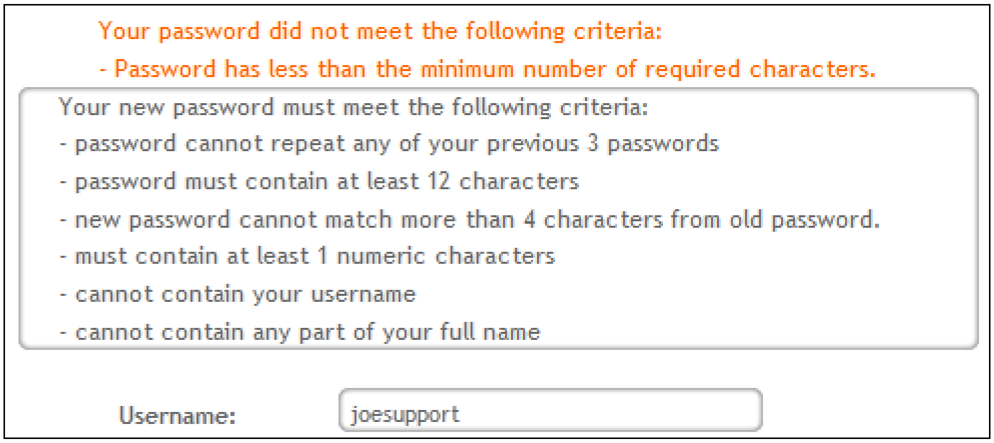
Old Password: ••••••••••••••••••••

New Password: ••••••••

Confirm New Password: ••••••••

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.



Your password did not meet the following criteria:

- Password has less than the minimum number of required characters.

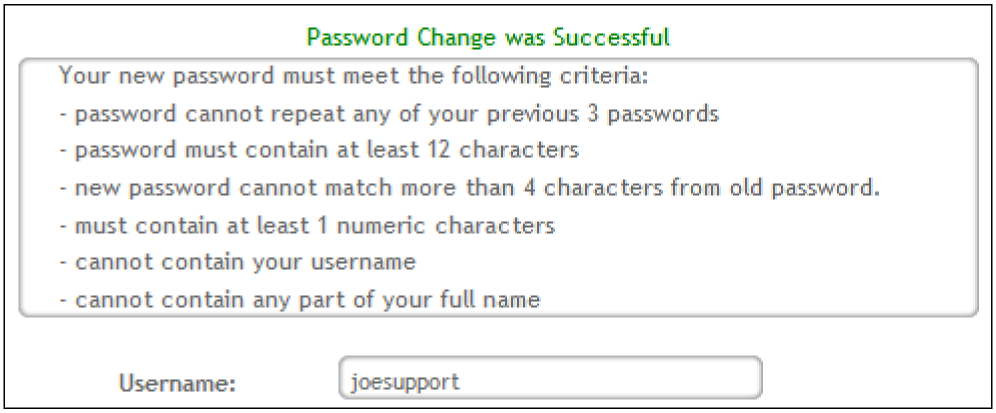
Your new password must meet the following criteria:

- password cannot repeat any of your previous 3 passwords
- password must contain at least 12 characters
- new password cannot match more than 4 characters from old password.
- must contain at least 1 numeric characters
- cannot contain your username
- cannot contain any part of your full name

Username: joesupport

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.



Password Change was Successful

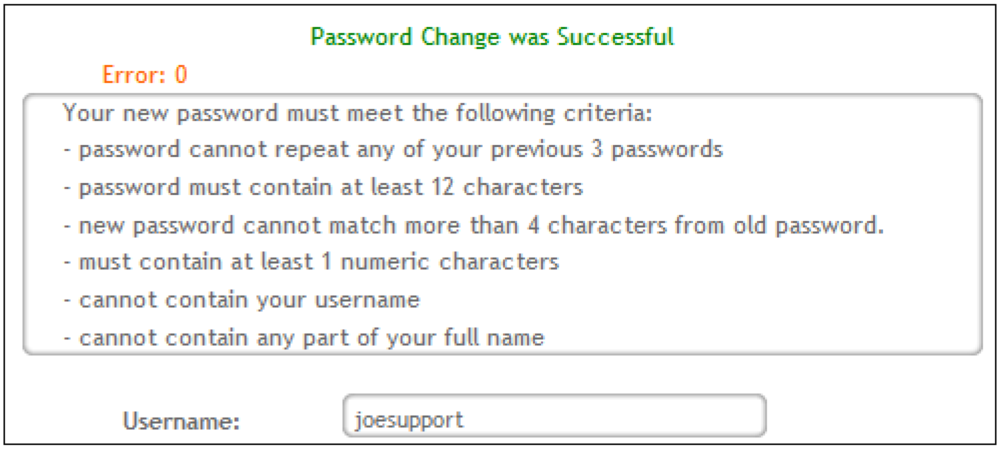
Your new password must meet the following criteria:

- password cannot repeat any of your previous 3 passwords
- password must contain at least 12 characters
- new password cannot match more than 4 characters from old password.
- must contain at least 1 numeric characters
- cannot contain your username
- cannot contain any part of your full name

Username: joesupport

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.



Password Change was Successful

Error: 0

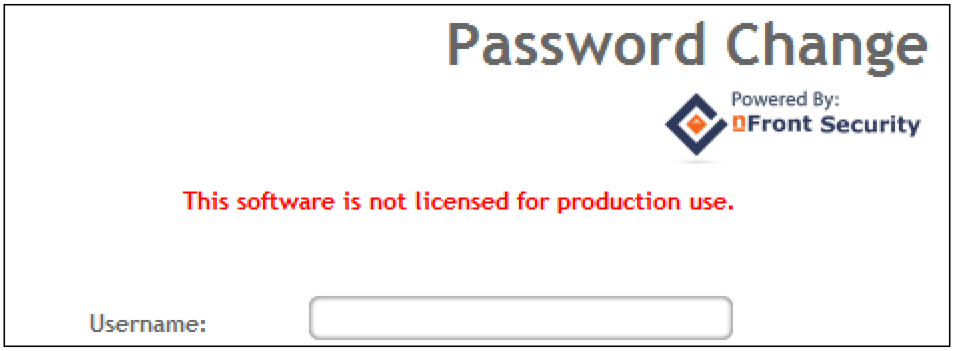
Your new password must meet the following criteria:
- password cannot repeat any of your previous 3 passwords
- password must contain at least 12 characters
- new password cannot match more than 4 characters from old password.
- must contain at least 1 numeric characters
- cannot contain your username
- cannot contain any part of your full name

Username: joesupport

Figure 3.6: Password change with debugging turned on.

4.0 Registering your evaluation copy

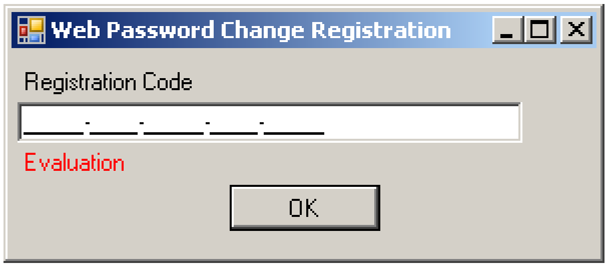
The evaluation copy will display a red text message above the password rules and username field. The message is not displayed on a licensed copy.



This software is not licensed for production use.

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.



_____-____-_____-____-_____

Evaluation

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 / Reason
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.
1351	The password change was not completed because the process is running under anonymous credentials. Please turn off Anonymous Authentication. 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	The password change was not completed because this process is running under the credentials of a trusted user outside of this domain. 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.