



WebFront for Service Manager Deployment Guide

Gridpro AB

Rev: 2.10.7509 (SCSM 2012 versions) & 3.0.7509 (SCSM 2016 & later)

Published: August 2020

Contents

Prerequisites	3
Windows Server	4
Server Configuration	4
Microsoft Silverlight 5 Installation (Optional)	7
Installation	8
WebFront for Service Manager.....	8
Active Directory Configuration (Only remote installation)	12
License Activation	14
Verify Installation.....	16
Upgrade	18
Remove obsolete Management Packs	20
Operations.....	21
Forms Authentication.....	21
Settings.....	22
Management Server	22
Set default Language	23
Force Language	24
Configure maximum initial rows returned.....	24
Automatically Refresh View On Submit.....	25
Forms Authentication Default Domain Name.....	25
Custom Branding	26
Deep Links	27
New Work Items	27
Existing Work Items and Configuration Items.....	27
WebFront Link	27
Form Customizations	28
Enabling Elevated Trust.....	28
CTI for Service Manager (Add-on)	33
Getting Started with Lync/Skype Integration	33
Getting started with Command line integration	36
Integration: Provance Asset Management.....	38
Uninstallation.....	39

Prerequisites

WebFront for Service Manager is a web interface for System Center Service Manager. A WebFront installation therefore requires a Microsoft System Center Service Manager installation in the environment to work properly.

Server Platform Requirements

- Minimum Microsoft Windows Server 2012
- Microsoft System Center 2012 Service Manager Console or later
- Web Server Role must be installed with the below minimum Web Server Role Services installed

Web Server Role Services					
Common HTTP Features	Application Development	Health and Diagnostics	Security	Performance	Management Tools
Static Content Default Document Directory Browsing HTTP Errors	ASP.NET 4.7* NET Extensibility 4.7* ISAPI Extensions ISAPI Filters	HTTP Logging Request Monitor	Windows Authentication Request Filtering	Static Content Compression Dynamic Content Compression	IIS Management Console IIS 6 Management Compatibility IIS 6 Metabase Compatibility
Features					
NET Framework 4.7 Features*		ASP.NET 4.7*			

* Version 4.5 on Windows Server 2012; Version 4.6 on Windows Server 2016; Version 4.7 on Windows Server 2019

Client Platform Requirements

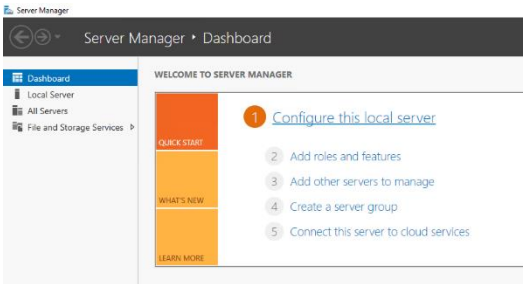
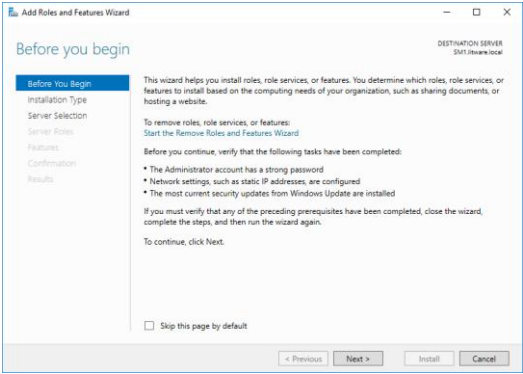
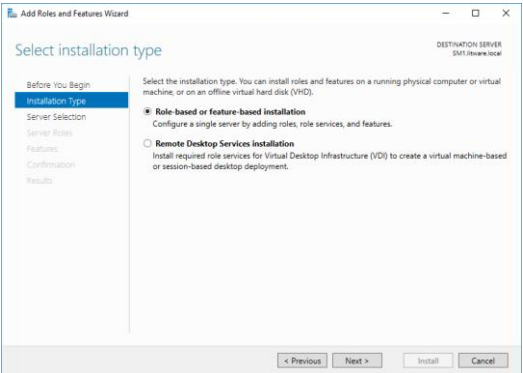
- Browsers
 - Internet Explorer 7 or later
 - Mozilla Firefox 3.6 or later
- Silverlight 5

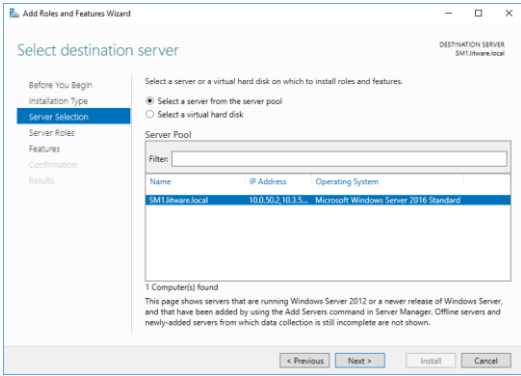
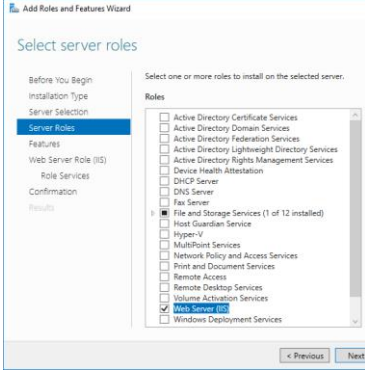
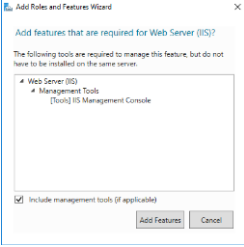
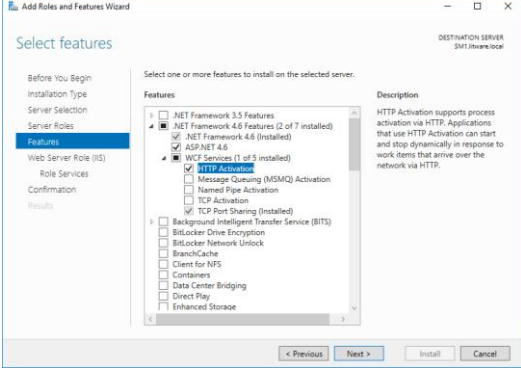
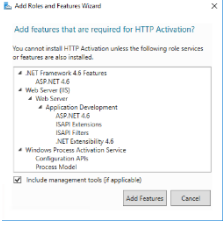
Important: If you are installing or upgrading WebFront in a Service Manager 2012 environment, please make sure you use a version that is lower than 3.0. If you are on Service Manager 2016 or later, please make sure you use an installer with a higher version number than 3.0. If you have any questions, please contact support@gridprosoftware.com.

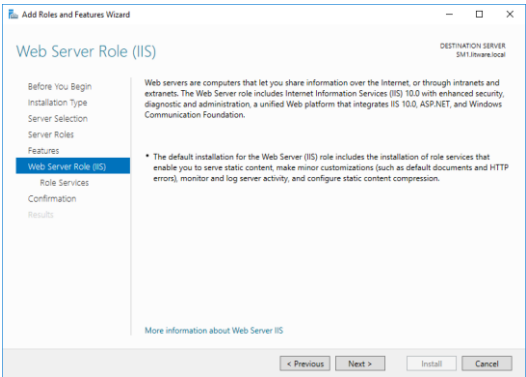
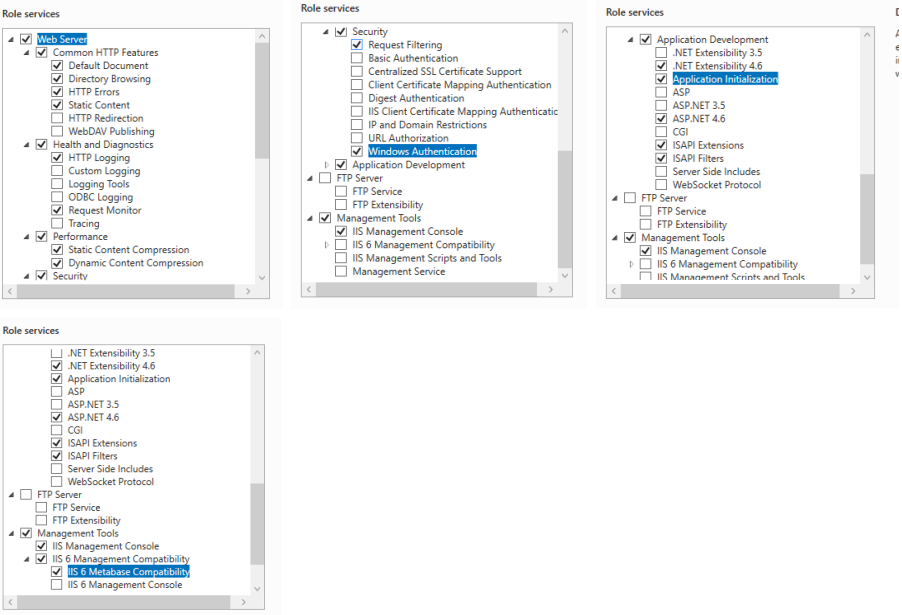
Windows Server

Server Configuration

The following section will describe the minimum Web Server Role Services that needs to be installed to enable WebFront to work correctly. On the server that will host WebFront for Service Manager, perform the following steps.

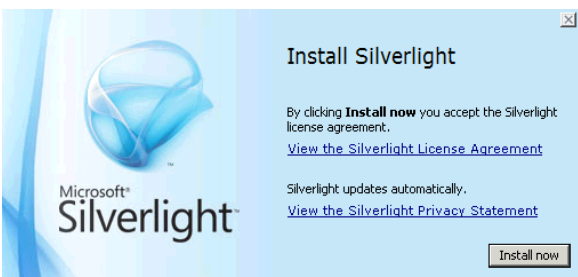
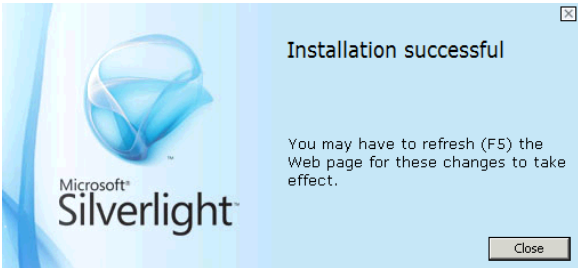
<input type="checkbox"/>	Click Start – Server Manager
<input type="checkbox"/>	 <p>Click Add Roles and features</p>
<input type="checkbox"/>	 <p>Click Next</p>
<input type="checkbox"/>	 <p>Click Next</p>

<input type="checkbox"/>		<p>Click Next</p>
<input type="checkbox"/>		<p>Check Web Server (IIS)</p>  <p>Click Add Features in popup, then click Next</p>
<input type="checkbox"/>	  <p>Click Next when finished</p>	<p>Check minimum required features according to the left screenshot</p> <p>Click Add features when the below wizard appears</p>

<input type="checkbox"/>	 <p>Click Next</p>
<input type="checkbox"/>	<p>Check Role features according to pictures below, then click Next</p> 
<input type="checkbox"/>	<p>Click Close</p>
<input type="checkbox"/>	<p>Close Server Manager console</p>

Microsoft Silverlight 5 Installation (Optional)

To be able to verify WebFront functionality using the web browser on the server, Silverlight 5 needs to be installed. This is optional and another computer that has Silverlight 5 installed can be used instead.

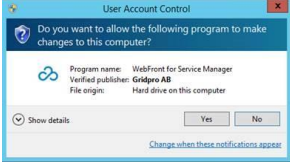
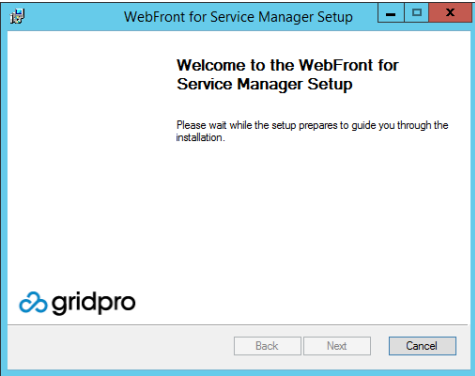
<input type="checkbox"/>	Download Silverlight 5 (Link) and save to a temporary location
<input type="checkbox"/>	Run Silverlight.exe
<input type="checkbox"/>	 Click Install now
<input type="checkbox"/>	 Click Close

Installation

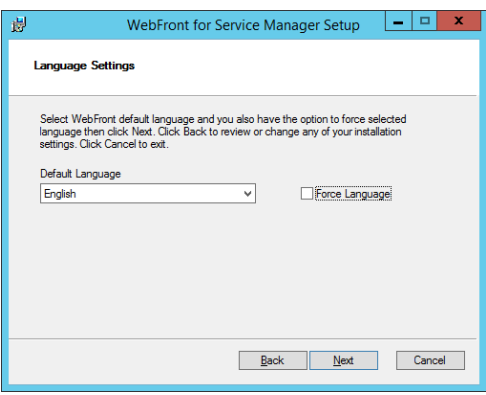
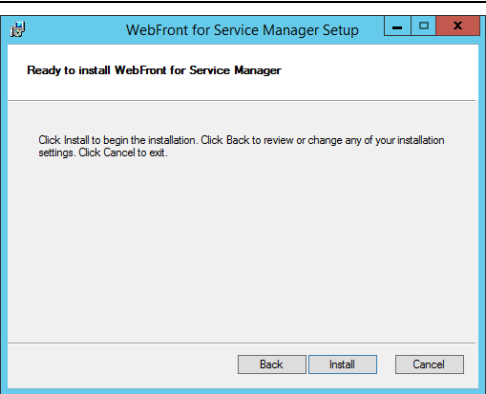
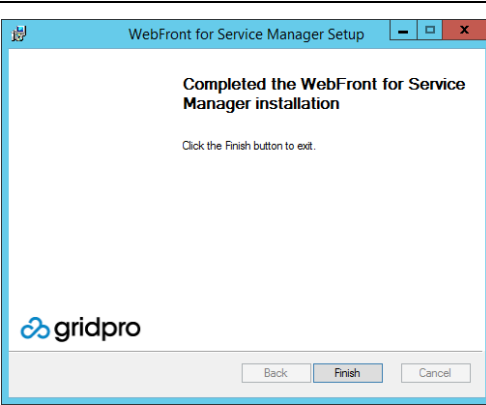
WebFront for Service Manager can be installed on the same server as the Service Manager Management server role as well as installed on a remote server. This section is a basic step-by-step instruction how to install WebFront for Service Manager software in both scenarios. The only difference is the Active Directory configuration that needs to be done in the remote server scenario.

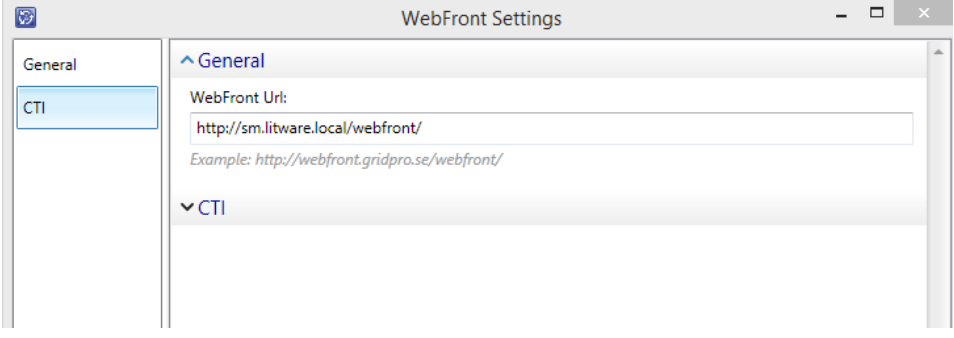
WebFront for Service Manager

WebFront for Service Manager Setup checks prerequisites if you get an error during setup please verify that you have fulfilled the prerequisites.

<input type="checkbox"/>	<p>IMPORTANT: Login using a user account that is a member of the local server administrator group and has been assigned the SCSM Administrator role in Service Manager.</p>
<input type="checkbox"/>	<p>Run WebFront for Service Manager vX.X.XXXX.exe</p>
<input type="checkbox"/>	<p>If <u>User Access Control</u> is enabled, click Yes</p> 
<input type="checkbox"/>	<p>Click Next</p> 
<p>NOTE:</p>	<p>If you receive an error message that states "Unable to retrieve IIS .NET 4 Application Pools.." this is because there are no application pools configured for .NET Framework 4 on the Web server. This is probably caused by that the Web server role was installed after .NET Framework 4 installation and no application pools was created by the .NET Framework 4 setup. These application pools can be created by repairing .NET Framework 4 installation. Follow the instructions below to correct the problem:</p> <ol style="list-style-type: none"> 1. Open Control Panel 2. Click Uninstall a Program 3. Select Microsoft .NET Framework 4 Extended 4. Click Uninstall/Change 5. Select Repair Microsoft .NET Framework 4 Extended to its original state then click Next

	<p>6. Click Finish</p> <p>7. Restart WebFront Setup and the error should not reoccur</p>
<input type="checkbox"/>	<div data-bbox="352 398 834 775" data-label="Image"> </div> <div data-bbox="855 398 1340 544" data-label="Text"> <p>Read Software License Agreement carefully and if you accept the terms check I accept the terms in the License Agreement, then click Next</p> </div>
<input type="checkbox"/>	<div data-bbox="347 817 834 1196" data-label="Image"> </div> <div data-bbox="855 817 1340 1021" data-label="Text"> <p>Click Next</p> <p>NOTE: Leave the default values if you don't have any specific requirements</p> </div>
<input type="checkbox"/>	<div data-bbox="347 1236 834 1615" data-label="Image"> </div> <div data-bbox="855 1236 1340 1339" data-label="Text"> <p>Specify Management Server fully qualified domain name (FQDN) servername, then click Next</p> </div>

<input type="checkbox"/>		<p>Select default language from dropdown list, then click Next</p>
<input type="checkbox"/>		<p>Click Install</p>
<input type="checkbox"/>		<p>Click Finish</p>
	<p>An additional last step is configuring the URL used by the WebFront Link tasks that allow you to get a direct URL to a Work Item or Configuration Items using a task in WebFront or the Standard Console.</p>	
<input type="checkbox"/>	<p>Click Start – All Programs – Microsoft System Center – Service Manager – Service Manager Console</p>	
<input type="checkbox"/>	<p>Click Administration tab</p>	
<input type="checkbox"/>	<p>In the right pane click Settings</p>	
<input type="checkbox"/>	<p>Double-click WebFront Settings in the middle pane</p>	

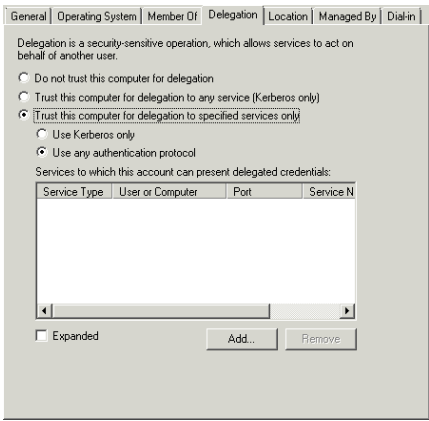
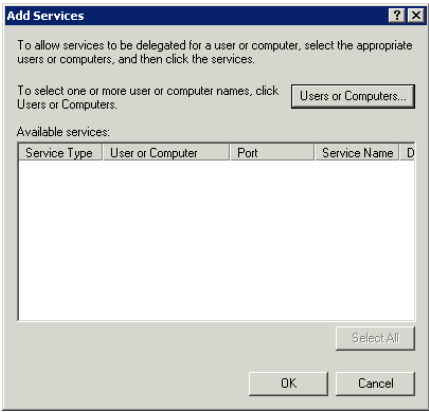


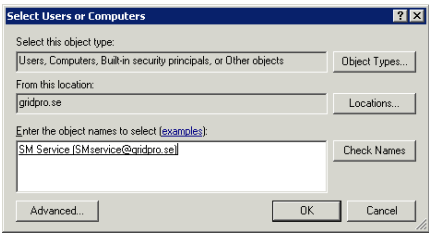
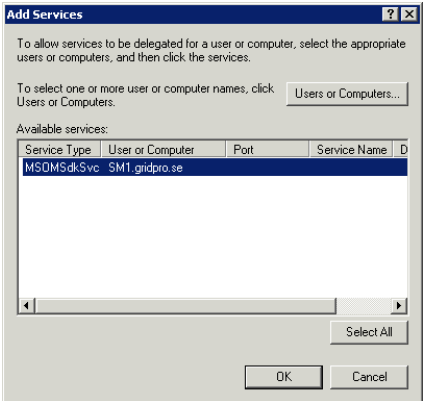
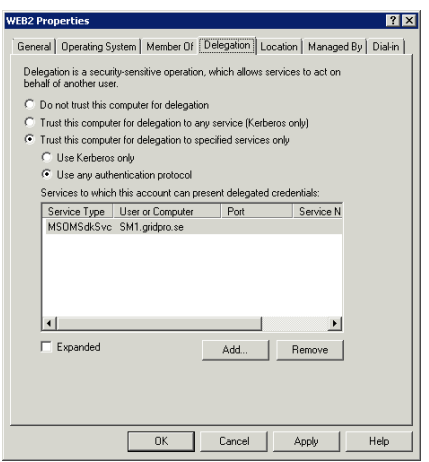
Type the URL to your WebFront site in the **WebFront URL** field. Then click **OK** to save the settings

IMPORTANT: URL needs to end with a trailing slash.

Active Directory Configuration (Only remote installation)

IMPORTANT: This step is only necessary if WebFront is installed on a separate server than the Service Manager Management server. Gridpro WebFront for Service Manager is performing an impersonation of the actual user when working against the Service Manager Management server. In other words, the user's credentials are used to access Service Manager. This way the normal security settings in Service Manager are implied in WebFront. So, the Service Management service account must be delegated the permission to be able to impersonate in Active Directory. The section below shows a step-by-step instruction how this is accomplished.

On a computer with Active Directory Users and Computers console installed	
<input type="checkbox"/>	Open Active Directory Users and Computers console
<input type="checkbox"/>	Find the Computer object for the server hosting WebFront for Service Manager
<input type="checkbox"/>	Right-Click Computer object and select Properties
<input type="checkbox"/>	Click Delegation tab
<input type="checkbox"/>	<div style="display: flex; align-items: flex-start;"> <div style="flex: 1;">  </div> <div style="flex: 1; padding-left: 10px;"> <p>Select Trust this computer for delegation to specified services only, then select Use any authentication protocol</p> </div> </div>
<input type="checkbox"/>	Click Add...
<input type="checkbox"/>	<div style="display: flex; align-items: flex-start;"> <div style="flex: 1;">  </div> <div style="flex: 1; padding-left: 10px;"> <p>Click Users or Computers...</p> </div> </div>

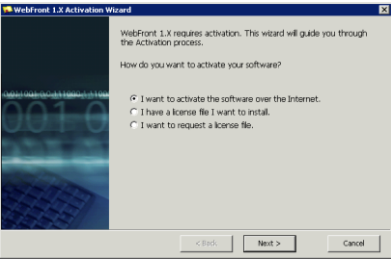
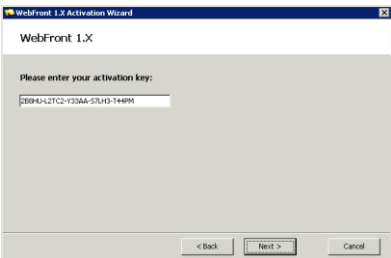
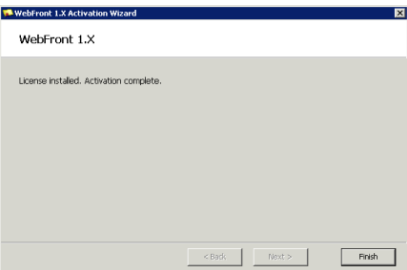
<input type="checkbox"/>		<p>Type in the name of the account that your Service Manager server are using for running the <i>System Center Data Access Service</i> service, click Check Names to verify the name and then click OK</p> <p>NOTE: If you are unsure about the account you can identify it by opening the Services snap-in, and connect to the Service Manager Management server and verify the account in the Log On As column for the System Center Data Access Service. If you are running as Local System you should select the computer account of the WebFront server.</p> <table border="1" data-bbox="304 757 1353 869"> <thead> <tr> <th>Name</th> <th>Description</th> <th>Stat</th> <th>Startup T</th> <th>Log On As</th> </tr> </thead> <tbody> <tr> <td>System Center Data Access Service</td> <td>Microsoft System Center Data Access Service.</td> <td>Started</td> <td>Automatic</td> <td>GRIDPRO\SMservice</td> </tr> <tr> <td>System Center Management</td> <td></td> <td>Started</td> <td>Automatic</td> <td>Local System</td> </tr> <tr> <td>System Center Management Configuration</td> <td>System Center Management Configuration Service</td> <td>Started</td> <td>Automatic</td> <td>GRIDPRO\SMservice</td> </tr> </tbody> </table>	Name	Description	Stat	Startup T	Log On As	System Center Data Access Service	Microsoft System Center Data Access Service.	Started	Automatic	GRIDPRO\SMservice	System Center Management		Started	Automatic	Local System	System Center Management Configuration	System Center Management Configuration Service	Started	Automatic	GRIDPRO\SMservice
Name	Description	Stat	Startup T	Log On As																		
System Center Data Access Service	Microsoft System Center Data Access Service.	Started	Automatic	GRIDPRO\SMservice																		
System Center Management		Started	Automatic	Local System																		
System Center Management Configuration	System Center Management Configuration Service	Started	Automatic	GRIDPRO\SMservice																		
<input type="checkbox"/>		<p>Select Service Type MSOMSdkSvc and click OK</p> <p>NOTE: If the Available services box is empty your configured service account running the System Center Data Access Service has not enough permission to register its SPN in Active Directory. Please correct the problem and retry this step.</p>																				
		<p>Click OK</p>																				
<input type="checkbox"/>	<p>Close Active Directory Users and Computers console</p>																					
<p>IMPORTANT: Wait for Active Directory change to replicate to all domain controllers in your domain before proceeding to next step. This can take up to an hour depending on your environment configuration</p>																						

<input type="checkbox"/>	Restart the server hosting WebFront for Service Manager to apply the delegation changes on the server

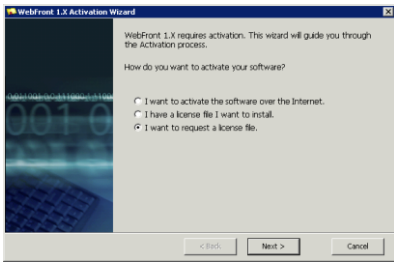
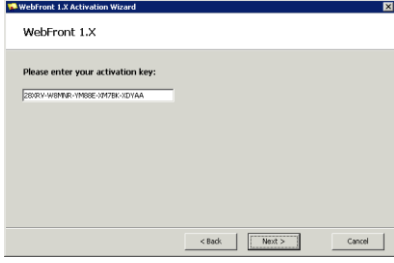
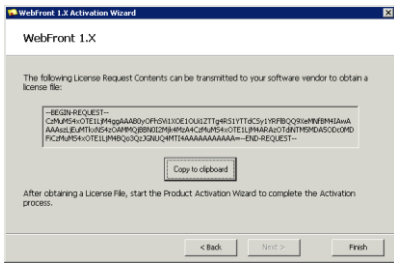
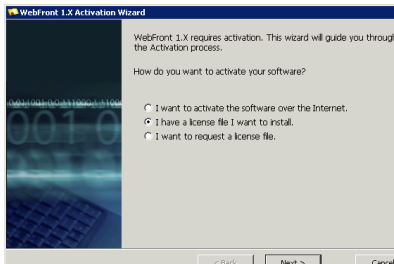
License Activation

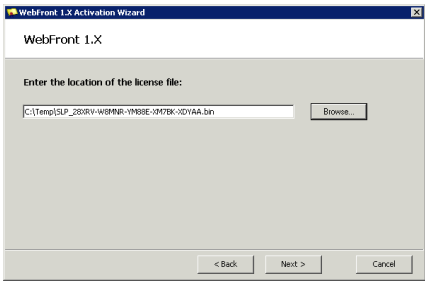
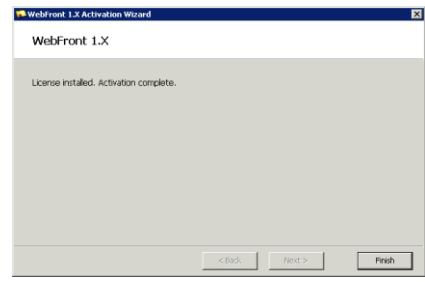
The section below shows a step-by-step instruction how this is accomplished. It's the same procedure for evaluation activation and commercial registration. When performing a commercial activation any active evaluation licenses will be automatically removed and replaced by commercial license.

Activation of server with Internet access

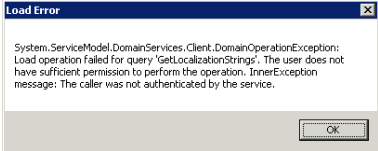
Do these steps on the WebFront server	
<input type="checkbox"/>	Click All Programs – WebFront for Service Manager – WebFront License Activation
<input type="checkbox"/>	 <p>Select I want to activate the software over the Internet, then click Next</p>
<input type="checkbox"/>	 <p>Specify Activation Key provided by Gridpro AB, then click Next</p>
<input type="checkbox"/>	 <p>Click Finish</p>
<input type="checkbox"/>	Close WebFront License Activation
<input type="checkbox"/>	Your license has now been activated and WebFront is ready

Activation of server without Internet access

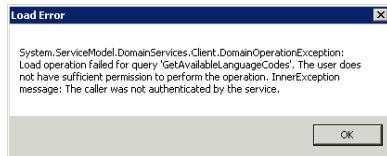
Do these steps on the WebFront server	
<input type="checkbox"/>	Click All Programs – WebFront for Service Manager – WebFront License Activation
<input type="checkbox"/>	 <p>Select I want to request a license file, then click Next</p>
<input type="checkbox"/>	 <p>Specify Activation Key provided by Gridpro AB, then click Next</p>
<input type="checkbox"/>	 <p>Click Copy to clipboard and paste the information into a text file. Save the text file for later use. Then click Finish</p>
<input type="checkbox"/>	Send the text file saved earlier as an attachment together with your Company name and Activation Code to support@gridprosoftware.com (you should receive a response within 24 hours).
<i><u>When you receive a response email containing a license file you can continue to next step.</u></i>	
<input type="checkbox"/>	Click All Programs – WebFront for Service Manager – WebFront License Activation
<input type="checkbox"/>	 <p>Select I have a license file I want to install, then click Next</p>
<input type="checkbox"/>	Click Browse and browse to the license file received from Gridpro AB and click Open

<input type="checkbox"/>		Click Next
<input type="checkbox"/>		Click Finish
<input type="checkbox"/>	Close WebFront License Activation	
<input type="checkbox"/>	Your license has now been activated and WebFront is ready	

Verify Installation

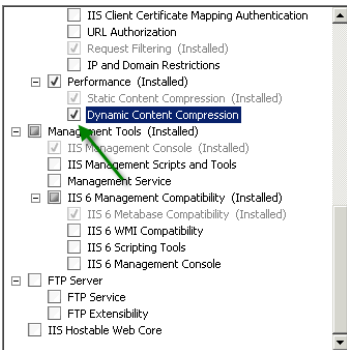
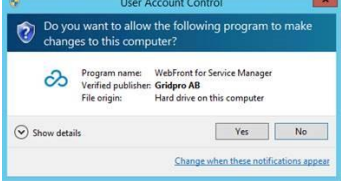
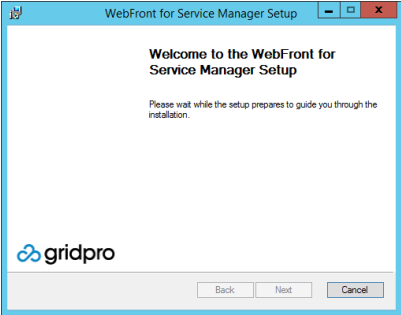
<p>This step can be made on any client in the domain that fulfills the client prerequisites. If you log on from a server operating system, you will always be prompted for credentials</p>	
<input type="checkbox"/>	Open your browser
<input type="checkbox"/>	<p>Type in <a href="http://<WebFrontServerName>/WebFront">http://<WebFrontServerName>/WebFront in address field and press Enter</p> <p>NOTE: Variable <WebFrontServerName> should be replaced by the WebFront Server name in your environment</p>
<input type="checkbox"/>	<p>WebFront for Service Manager should now start, and be ready for work.</p> <p>Common Errors</p> <p><u>Symptoms:</u> When you enter WebFront you get similar error message as shown below.</p> 

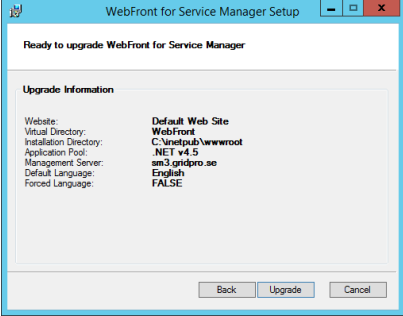
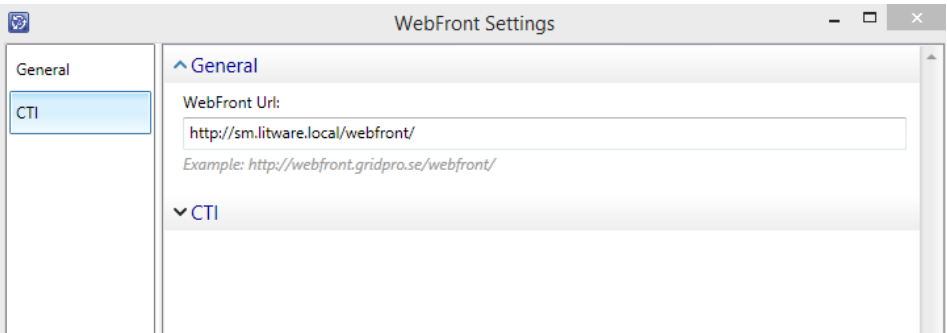
Solution: Delegation configuration does not work correctly. Please go through the *Active Directory Configuration* section again and verify your environment.



Upgrade

This section describes the procedure to upgrade any previous version of WebFront for Service Manager to the latest version.

<input type="checkbox"/>	IMPORTANT: Login using a user account that is a member of the local server administrator group and has been assigned the SCSM Administrator role in Service Manager.
<input type="checkbox"/>	Click Start – All Programs – Administrative Tools – Server Manager
<input type="checkbox"/>	Select Roles in the left-pane
<input type="checkbox"/>	In the right-pane select Add Role Services in the Web Server (IIS) section
<input type="checkbox"/>	 <p>Verify if Dynamic Content Compression is checked. If not, check Dynamic Content Compression and then click Next</p>
<input type="checkbox"/>	Click Install
<input type="checkbox"/>	Click Close
<input type="checkbox"/>	Close Server Manager
<input type="checkbox"/>	Run WebFront for Service Manager vX.X.XXXX.exe
<input type="checkbox"/>	 <p>If <u>User Access Control</u> is enabled, click Yes</p>
<input type="checkbox"/>	 <p>Click Next</p>

<input type="checkbox"/>		Review configuration data and click Upgrade
<input type="checkbox"/>	Click Finish	
To verify that the URL used by the WebFront Link tasks that allow you to get a direct URL to a Work Item or CI using a task in WebFront or the Standard Console is configured.		
<input type="checkbox"/>	Click Start – All Programs – Microsoft System Center – Service Manager – Service Manager Console	
<input type="checkbox"/>	Click Administration tab	
<input type="checkbox"/>	In the right pane click Settings	
<input type="checkbox"/>	Double-click WebFront Settings in the middle pane	
<input type="checkbox"/>		Verify that the URL to your WebFront site is specified in the WebFront URL field, if not type in the WebFront site. Then click OK to save the settings

Remove obsolete Management Packs

If you have upgraded from a previous version of WebFront for Service Manager you should follow the steps below to make sure you clean out obsolete Management Packs.



After verifying that all form customizations have been properly upgraded, if you have any of the following Management Packs in your environment, these are obsolete and can be deleted.

- `Gridpro.WebFront.ServiceManager.Customization.Configuration`
- `Gridpro.WebFront.ServiceManager.Customization.Library`

IMPORTANT

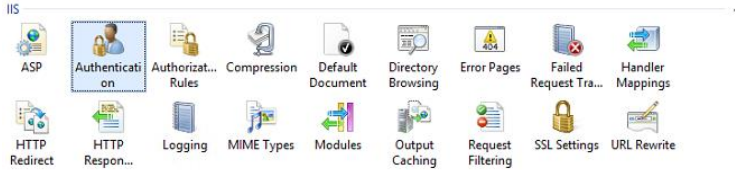
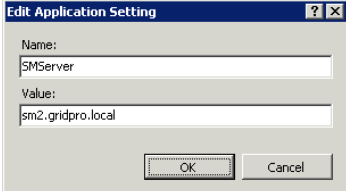
The management pack

`Gridpro.WebFront.ServiceManager.Customization.Configuration` contains custom form customizations that were created in older versions of WebFront. The upgrade should already have migrated these settings, but as an extra precaution please do an export copy of the MP's before deleting them.

Operations

Forms Authentication

By default, WebFront for Service Manager uses Windows Authentication, this provides a smooth single-sign-on experience for the WebFront users. WebFront supports an alternative login method called Forms Authentication which will allow you to prompt the user for a login name and password, this can be useful if you want users to be able to login using a different account than the one they are logged into the computer with. Using Forms Authentication also allows users to switch account by clicking a Sign Out button. To change the authentication method to Forms Authentication, follow these steps.

1.	Click Start – Administrative Tools – Internet Information Services (IIS) Manager																		
2.	Expand <WEBSERVER> - Sites - <WEBSITE> - <WEBFRONTDIR>																		
3.	 <p>Right-Click Authentication and select Open Feature</p>																		
4.	<table border="1"> <thead> <tr> <th>Name</th> <th>Status</th> <th>Response Type</th> </tr> </thead> <tbody> <tr> <td>Anonymous Authentication</td> <td>Enabled</td> <td></td> </tr> <tr> <td>ASP.NET Impersonation</td> <td>Disabled</td> <td></td> </tr> <tr> <td>Basic Authentication</td> <td>Disabled</td> <td>HTTP 401 Challenge</td> </tr> <tr> <td>Forms Authentication</td> <td>Enabled</td> <td>HTTP 302 Login/Redirect</td> </tr> <tr> <td>Windows Authentication</td> <td>Disabled</td> <td>HTTP 401 Challenge</td> </tr> </tbody> </table> <p>Make sure Anonymous- and Forms Authentication are the only Enabled and all others are Disabled</p>	Name	Status	Response Type	Anonymous Authentication	Enabled		ASP.NET Impersonation	Disabled		Basic Authentication	Disabled	HTTP 401 Challenge	Forms Authentication	Enabled	HTTP 302 Login/Redirect	Windows Authentication	Disabled	HTTP 401 Challenge
Name	Status	Response Type																	
Anonymous Authentication	Enabled																		
ASP.NET Impersonation	Disabled																		
Basic Authentication	Disabled	HTTP 401 Challenge																	
Forms Authentication	Enabled	HTTP 302 Login/Redirect																	
Windows Authentication	Disabled	HTTP 401 Challenge																	
5.	 <p>Change the Value to the fully qualified domain name for the the new Management Server, then click OK</p>																		
6.	Close Internet Information Services (IIS) Manager																		
7.	Go to the WebFront installation directory, typically "C:\inetpub\wwwroot\WebFront"																		
8.	Open the web.config file																		
9.	Find the following two sections:																		

	<pre> <basicHttpBinding> <binding name="HttpEndpointBinding" maxBufferSize="2147483647" maxReceivedMessageSiz <readerQuotas maxStringContentLength="2147483647" maxArrayLength="2147483647" /> <security mode="TransportCredentialOnly"> <!--Remove line below when using Forms Authentication--> <transport clientCredentialType="Windows" /> </security> </binding> <binding name="HttpEndpointBindingSSL" maxBufferSize="2147483647" maxReceivedMessageSiz <readerQuotas maxStringContentLength="2147483647" maxArrayLength="2147483647" /> <security mode="Transport"> <!--Remove line below when using Forms Authentication--> <transport clientCredentialType="Windows" /> </security> </binding> </basicHttpBinding> </pre> <p>Modify them, so they look like this:</p> <pre> <basicHttpBinding> <binding name="HttpEndpointBinding" maxBufferSize="2147483647" maxReceivedMessageSiz <readerQuotas maxStringContentLength="2147483647" maxArrayLength="2147483647" /> <security mode="TransportCredentialOnly"> <!--Remove line below when using Forms Authentication--> <!--<transport clientCredentialType="Windows" />--> </security> </binding> <binding name="HttpEndpointBindingSSL" maxBufferSize="2147483647" maxReceivedMessage! <readerQuotas maxStringContentLength="2147483647" maxArrayLength="2147483647" /> <security mode="Transport"> <!--Remove line below when using Forms Authentication--> <!--<transport clientCredentialType="Windows" />--> </security> </binding> </basicHttpBinding> </pre>
10.	<p>Save and close web.config</p> <p><i>Note: Due to directory permissions, you might need to save the file to an alternative location and copy the file back into the directory</i></p>
11.	<p>Finished</p>

Settings

Gridpro WebFront settings are stored as web application settings. These settings are configurable after installation using Internet Information Services (IIS) Manager.

Management Server

1.	Start notepad.exe as Administrator
2.	Click File – Open...
3.	Select %WebFront Installation Dir%\CustomSettings.config and click Open <i>Typically, "C:\inetpub\wwwroot\WebFront\CustomSettings.config"</i>
4.	To modify which Service Manager Management Server that is used by WebFront for Service Manager, change value of the <u>SMServer</u> setting (underlined in the example below).

	<add key="SMServer" value=" <u>scsm.contoso.com</u> " />
5.	Click File – Save and then Close Notepad
6.	Finished

Set default Language

1.	Start notepad.exe as Administrator																								
2.	Click File – Open...																								
3.	Select %WebFront Installation Dir%\CustomSettings.config and click Open <i>Typically, "C:\inetpub\wwwroot\WebFront\CustomSettings.config"</i>																								
4.	<p>To modify which language that should be used by default by WebFront for Service Manager, change value of the DefaultUserLanguageCode setting (underlined in the example below).</p> <pre><add key="DefaultUserLanguageCode" value="<u>ENU</u>" /></pre> <p>Change the Value to the three character code that reflects the language that you want to set as the WebFront default (see below table).</p> <table border="1" data-bbox="316 1205 916 1527"> <tr> <td>FRA - French</td> <td>ESN - Spanish (Spain)</td> <td>ENU - English</td> </tr> <tr> <td>SVE - Swedish</td> <td>ELL - Greek</td> <td>NOR - Norwegian</td> </tr> <tr> <td>CSY - Czech</td> <td>KOR - Korean</td> <td>RUS - Russian</td> </tr> <tr> <td>PTB - Portuguese</td> <td>DAN - Danish</td> <td>FIN - Finnish</td> </tr> <tr> <td>JPN - Japanese</td> <td>PTG - Portuguese (Portugal)</td> <td>PLK - Polish</td> </tr> <tr> <td>ITA - Italian</td> <td>CHT - Chinese (Taiwan)</td> <td>TRK - Turkish</td> </tr> <tr> <td>DEU - German</td> <td>CHS - Chinese (Simplified)</td> <td>NLD - Dutch</td> </tr> <tr> <td>HUN - Hungary</td> <td>ZHH - Chinese (Kantonese)</td> <td></td> </tr> </table>	FRA - French	ESN - Spanish (Spain)	ENU - English	SVE - Swedish	ELL - Greek	NOR - Norwegian	CSY - Czech	KOR - Korean	RUS - Russian	PTB - Portuguese	DAN - Danish	FIN - Finnish	JPN - Japanese	PTG - Portuguese (Portugal)	PLK - Polish	ITA - Italian	CHT - Chinese (Taiwan)	TRK - Turkish	DEU - German	CHS - Chinese (Simplified)	NLD - Dutch	HUN - Hungary	ZHH - Chinese (Kantonese)	
FRA - French	ESN - Spanish (Spain)	ENU - English																							
SVE - Swedish	ELL - Greek	NOR - Norwegian																							
CSY - Czech	KOR - Korean	RUS - Russian																							
PTB - Portuguese	DAN - Danish	FIN - Finnish																							
JPN - Japanese	PTG - Portuguese (Portugal)	PLK - Polish																							
ITA - Italian	CHT - Chinese (Taiwan)	TRK - Turkish																							
DEU - German	CHS - Chinese (Simplified)	NLD - Dutch																							
HUN - Hungary	ZHH - Chinese (Kantonese)																								
5.	Click File – Save and then Close Notepad																								
6.	Finished																								

Force Language

1.	Start notepad.exe as Administrator
2.	Click File – Open...
3.	Select %WebFront Installation Dir%\CustomSettings.config and click Open <i>Typically, "C:\inetpub\wwwroot\WebFront\CustomSettings.config"</i>
4.	To control if a user should be allowed to change to a language other than the default language in WebFront for Service Manager, change value of the DefaultUserLanguageCodelsMandatory setting (underlined in the example below). <pre><add key="DefaultUserLanguageCodelsMandatory" value="False" /></pre> <p>Change the Value to <i>TRUE</i> to enforce the use of Default Language. The end-user will not be able to change language in WebFront. <i>FALSE</i> is the default value.</p>
5.	Click File – Save and then Close Notepad
6.	Finished

Configure maximum initial rows returned

1.	Start notepad.exe as Administrator
2.	Click File – Open...
3.	Select %WebFront Installation Dir%\CustomSettings.config and click Open <i>Typically, "C:\inetpub\wwwroot\WebFront\CustomSettings.config"</i>
4.	To control the number of rows initially returned by a view in WebFront for Service Manager, change value of the InitialLoadSize setting (underlined in the example below). <pre><add key="InitialLoadSize" value="250" /></pre> <p>Do not increase this value before testing it in test environment, increasing the value could cause performance issues for end-users.</p>
5.	Click File – Save and then Close Notepad
6.	Finished

Automatically Refresh View On Submit

When submitting changes made to an object in a form or using a console task, WebFront does not automatically refresh the selected view. To force WebFront to update the selected view after making changes to a work item or configuration item, follow these steps.

1.	Start notepad.exe as Administrator
2.	Click File – Open...
3.	Select %WebFront Installation Dir%\CustomSettings.config and click Open <i>Typically, "C:\inetpub\wwwroot\WebFront\CustomSettings.config"</i>
4.	To enable "auto refresh", change value of the AutoRefreshViewOnSubmit setting (underlined in the example below) to <i>TRUE</i> . The default value is <i>FALSE</i> . <add key=" AutoRefreshViewOnSubmit " value=" <u>False</u> " />
5.	Click File – Save and then Close Notepad
6.	Finished

Forms Authentication Default Domain Name

When using **Forms Authentication**, you have the possibility to set a default domain name. This will prepopulate "<domain name>\" in the username textbox so the user only needs to add their username instead of having to type "domain\username". To do so, follow these steps.

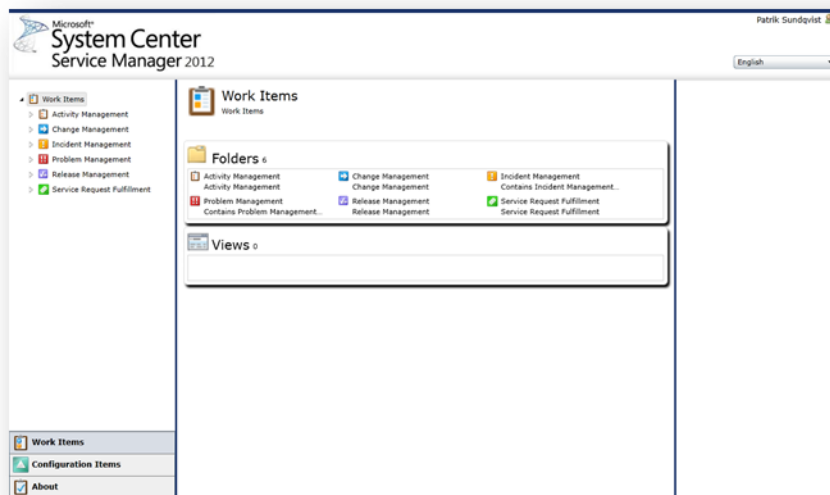
1.	Start notepad.exe as Administrator
2.	Click File – Open...
3.	Select %WebFront Installation Dir%\CustomSettings.config and click Open <i>Typically, "C:\inetpub\wwwroot\WebFront\CustomSettings.config"</i>
4.	To set a default domain name, change value of the FormsAuthenticationDefaultDomainName setting (see example below). The default value is empty. <add key=" FormsAuthenticationDefaultDomainName " value="" />
5.	Click File – Save and then Close Notepad
6.	Finished

Custom Branding

Customer branding functionality in WebFront enables customers to replace parts of the Gridpro branding images with custom company images.

	Image requirements <ul style="list-style-type: none"> • PNG format • Transparent Background • 90 Pixels Maximum Height
	<u>Replacing Top Left Image</u>
1.	Rename your PNG image file to: top_left_logo_90.png
2.	Copy top_left_logo_90.png the folder %WebFrontDir%\ClientBin\CustomTheme
	<u>Replacing Top Center Image</u>
1.	Rename your PNG image file to: top_center_symbol_90.png
2.	Copy top_center_symbol_90.png the folder %WebFrontDir%\ClientBin\CustomTheme

See example below where both images have been rebranded. To hide a logo or symbol copy a blank PNG file.



Deep Links

WebFront contains functionality to spawn new as well as access existing work items using deep links.

New Work Items

Using a link with SpawnType parameter new work item form will open for spawn work item type. This could for example be useful when you want to publish a link on your intranet for registering new Incidents etc.

Supported Work items:

- Incident
- Change
- Problem

Example: <http://web1.gridpro.se/WebFront/WebConsole.aspx?SpawnType=Incident>

Existing Work Items and Configuration Items

Using a URL containing an Object GUID any work item or configuration item can be accessed directly. This could for example be injected as a property in a Service Manager Notification template e-mail, providing the recipient direct access to a work item or configuration item through the web browser. To inject Object GUID into the notification template use `$Context/?$Id$?` .

Example: <http://web1.gridpro.se/WebFront/WebConsole.aspx?InternalId=1cd53de22-d49b-a3fd-01fd-1fc049c37daa1>

WebFront Link

To simplify retrieving the deep link for a work item or configuration item, a console task is included in the WebFront Management Pack (see picture below). The console task can be used to open a browser window showing the currently selected item in WebFront.



Form Customizations

Please see WebFront Authoring Guide.

Enabling Elevated Trust

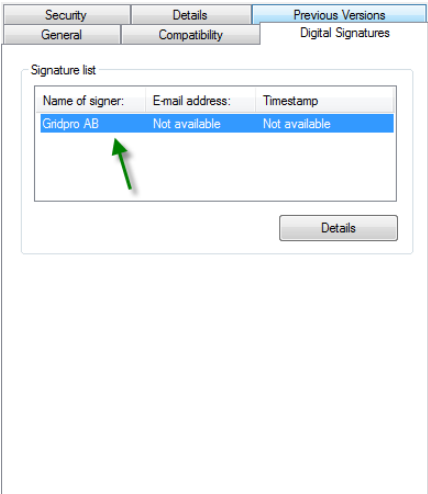
By configuring elevated trust for WebFront for Service Manager you enable the following features:

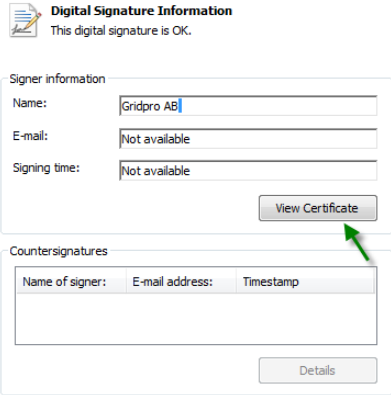
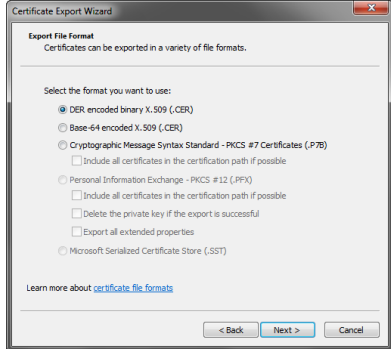
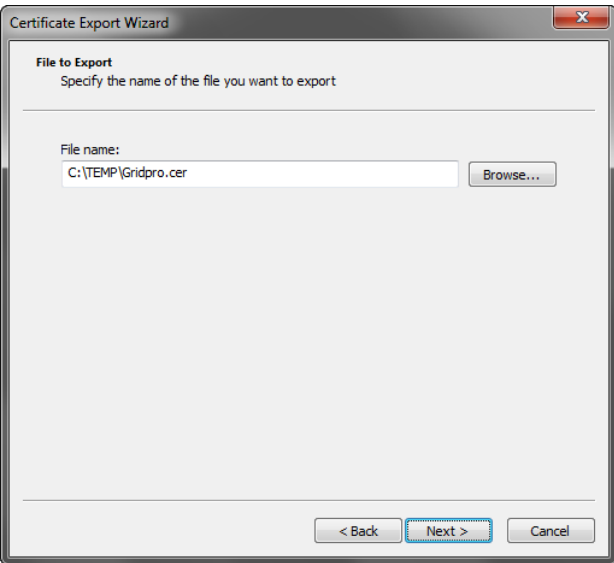
- Allow WebFront to directly open File Attachments instead of the standard behavior that files need to be saved locally before opened.
- Allow WebFront to show and execute console tasks that have been created through the standard console (Library > Tasks).

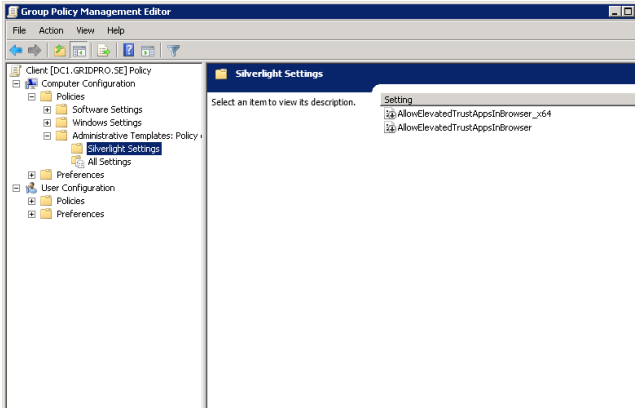
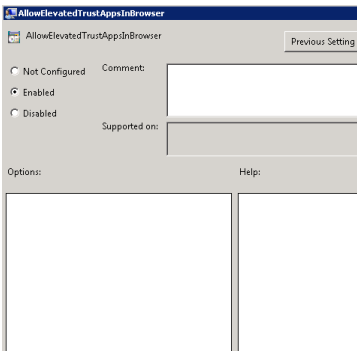
To enable these, two modifications need to be made on the end-user clients:

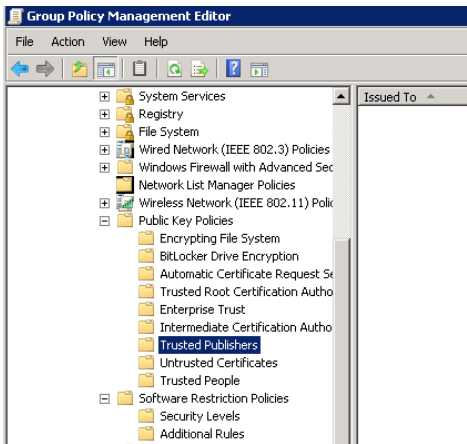
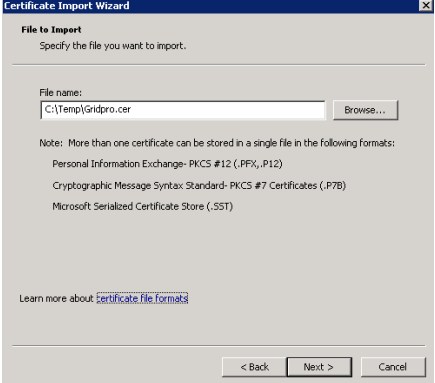
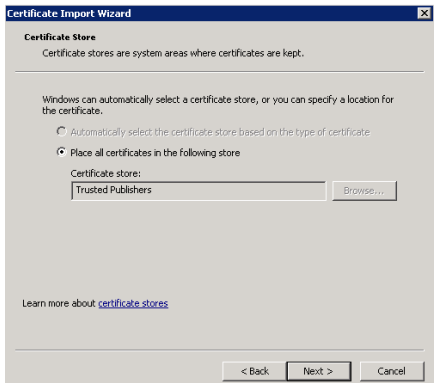
- The DWORD registry key AllowElevatedTrustAppsInBrowser needs to be set to 1 (HKLM\Software\Wow6432Node\Microsoft\Silverlight and HKLM\Software\Microsoft\Silverlight for 64-bit clients)
- Gridpro AB certificate needs to be added to Trusted Publishers folder in the local machine certificate store.

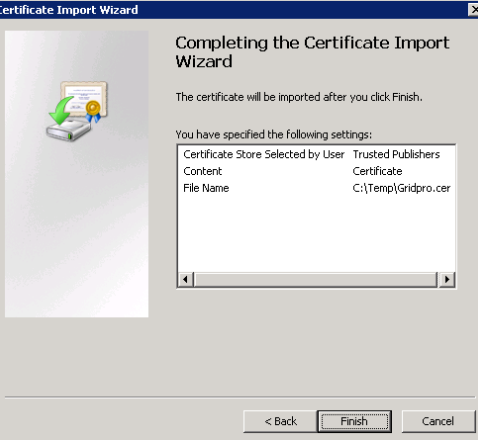
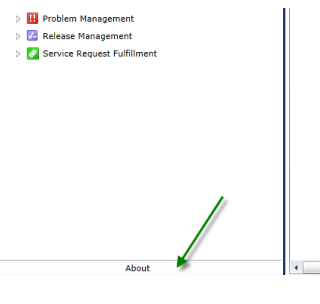

This can be done manually or distributed as software package. Another option is to apply the setting through Active Directory Group policy, and that is what is described below in a Windows Active Directory environment. If you are using one of the two first alternatives, you can follow the steps 1 to 7 to extract the certificate file.

1.	Right-Click WebFront for Service Manager vX.X.XXXX.exe and select Properties
2.	 <p>Click Digital Signatures Tab, then select Gridpro AB</p> <p>Then click Details</p>

3.	<div style="display: flex; justify-content: space-between;"> <div data-bbox="343 331 735 723">  </div> <div data-bbox="767 315 1031 344">Click View Certificate</div> </div>
4.	Click Details Tab and then click Copy to File...
5.	<div style="display: flex; justify-content: space-between;"> <div data-bbox="343 846 735 1193">  </div> <div data-bbox="759 846 1310 909">Select DER encoded binary x.509 (.CER) then click Next</div> </div>
6.	<div style="display: flex; justify-content: space-between;"> <div data-bbox="327 1249 943 1809">  </div> <div data-bbox="963 1240 1318 1379">Type a temporary path and filename for exported certificate (you will need this file later)</div> </div> <p style="margin-top: 20px;">Click Next</p>
7.	Click Finish
8.	Click OK

9.	Extract <code>%DRIVE%\Inetpub\wwwroot\WebFront\Bin\Gridpro_GPO_Templates.zip</code> to a temporary location
10.	Copy <code>GridproApplicationSettings.admx</code> and folder <code>en-US</code> to your Group Policy Central Store (<code>\\%FQDN%\SYSVOL\%FQDN%\policies\PolicyDefinitions</code>)
11.	Open Group Policy Management Editor
12.	Create a new Group Policy or edit an existing Group Policy that is applied on the clients.
13.	 <p data-bbox="975 669 1315 808">Expand Computer Configuration – Policies – Administrative Templates – Silverlight Settings</p>
14.	Depending on the target clients double-click <code>AllowElevatedTrustAppsInBrowser</code> or <code>AllowElevatedTrustAppsInBrowser_x64</code> (You can repeat step 14-15 for both if you have a mixed environment)
15.	 <p data-bbox="703 1261 1054 1290">Select Enabled and click OK</p>

16.		Expand Computer Configuration – Policies – Windows Settings – Security Settings – Public Key Policies –Trusted Publishers
17.	Right-click Trusted Publishers node and select Import...	
18.	Click Next	
19.		Type in the path to the exported certificate exported in step 6
		Then click Next
20.		Verify that Trusted Publisher is selected as Certificate Store
		Then click Next

21.		Click Finish
22.	Close Group Policy Management Editor	
23.	Verify that the settings is applied by opening WebFront from the client	
24.		Click About
25.		Verify that Has elevated permission is set to True

CTI for Service Manager (Add-on)

CTI for Service Manager enables Service Manager Integration with Lync (or Skype for Business) as well as generic switchboards that have client software that is capable of executing a command line with input parameters such as phone number or sip.

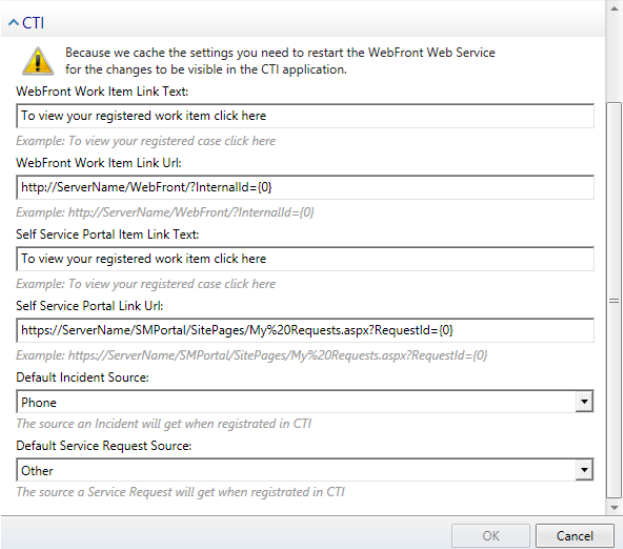
This document will only describe the process of configuring the Lync/Skype integration. But if you want to configure it for your generic switchboard, please contact our support at: support@gridprosoftware.com and they will assist you with the process.

Getting Started with Lync/Skype Integration

Prerequisites

- Lync 2013 Client/Skype for Business 2015 Client or later
- Phone number populated in CMDB to be able to match incoming call with user in CMDB
- SIP or Email populated in CMDB to match incoming IM session in Lync with user in CMD

Configure Server CTI Settings

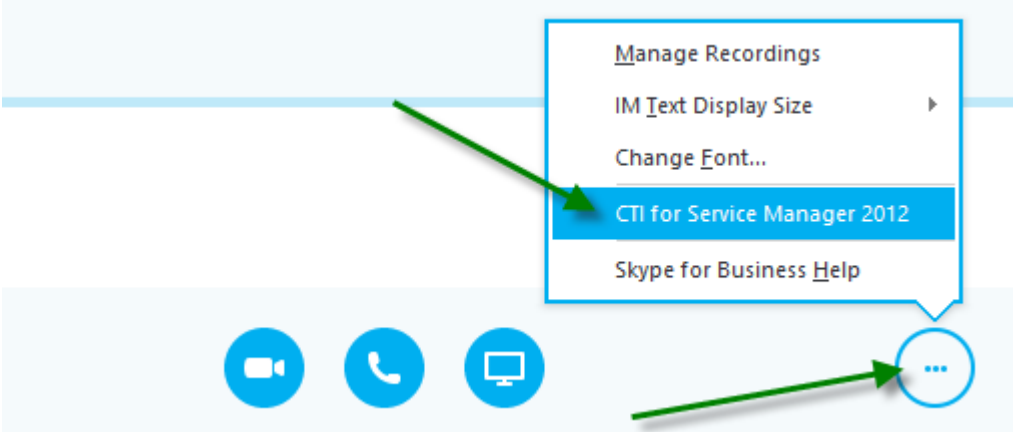
<input type="checkbox"/>	Click Start – All Programs – Microsoft System Center – Service Manager – Service Manager Console
<input type="checkbox"/>	Click Administration tab
<input type="checkbox"/>	In the right pane click Settings , Double-click WebFront Settings in the middle pane
<input type="checkbox"/>	<p>In the CTI section please configure the following:</p>  <ul style="list-style-type: none">• In the WebFront Work Item Link Url field replace <i>ServerName</i> with your WebFront server name

	<ul style="list-style-type: none"> In the Self-Service Portal Item Link Url field replace <i>ServerName</i> with your SCSM Self-Service portal server name
<input type="checkbox"/>	Click OK

Configure Client CTI Settings

Applying the settings on the Lync clients to enable the embedded experience requires registry settings to be applied to the HKEY_CURRENT_USER part of the registry.

On a server or client with Service Manager console installed	
	For Lync 2010 - Save the following text in a file with .reg extension
<input type="checkbox"/>	<pre>Windows Registry Editor Version 5.00 [HKEY_CURRENT_USER\Software\Microsoft\Communicator\ContextPackages\AFCFDg12-E1B7-4CB4-92EE-174D5E7A35DD] 'Name'='CTI for Service Manager' 'ExtensibilityWindowSize'=dword:00000000 'ExtensibilityApplicationType'=dword:00000001 'InternalURL'='http://<server>/WebFront/CTI.aspx' 'ExternalURL'='http://<server>/WebFront/CTI.aspx' 'ExtensibleMenu'='MainWindowActions;MainWindowRightClick;ConversationWindowActions;ConversationWindowRightClick;ContactCardMenu' [HKEY_CURRENT_USER\Software\Microsoft\Office\Lync\Security\Trusted Sites\<server>] 'http'=dword:00000001 'https'=dword:00000001</pre>
<input type="checkbox"/>	Replace all occurrences of <server> with the name of the WebFront server
	For Lync/Skype 2013 or later (64-bit) - Save the following text in a file with .reg extension
<input type="checkbox"/>	<pre>Windows Registry Editor Version 5.00 [HKEY_CURRENT_USER\Software\Microsoft\Office\<version>\Lync\Addins\AFCFDg12-E1B7-4CB4-92EE-174D5E7A35DD] 'Name'='CTI for Service Manager' 'ExtensibilityWindowSize'=dword:00000000 'ExtensibilityApplicationType'=dword:00000001 'InternalURL'='http://<server>/WebFront/CTI.aspx' 'ExternalURL'='http://<server>/WebFront/CTI.aspx' 'ExtensibleMenu'='MainWindowActions;MainWindowRightClick;ConversationWindowActions;ConversationWindowRightClick;ContactCardMenu' [HKEY_CURRENT_USER\Software\Microsoft\Office\Lync\Security\Trusted Sites\<server>] 'http'=dword:00000001 'https'=dword:00000001</pre>

<input type="checkbox"/>	<p>Replace all occurrences of <server> with the name of the WebFront server and <version> with the corresponding Lync/Skype version.</p> <p>2013 = 15.0 2016 = 16.0</p>
	<p>For Lync /Skype 2013 or later (32-bit) - Save the following text in a file with .reg extension</p>
<input type="checkbox"/>	<pre>Windows Registry Editor Version 5.00 [HKEY_CURRENT_USER\Software\Wow6432Node\Microsoft\Office\<version>\Lync\Addins\IAFCFDg12-E1B7-4CB4-g2EE-174D5E7A35DD] 'Name'='CTI for Service Manager' 'ExtensibilityWindowSize'=dword:00000000 'ExtensibilityApplicationType'=dword:00000001 'InternalURL'='http://<server>/WebFront/CTI.aspx' 'ExternalURL'='http://<server>/WebFront/CTI.aspx' 'ExtensibleMenu'='MainWindowActions;MainWindowRightClick;ConversationWindowActions;ConversationWindowRightClick;ContactCardMenu' [HKEY_CURRENT_USER\Software\Wow6432Node\Microsoft\Office\Lync\Security\Trusted Sites\<server>] 'http'-dword:00000001 'https'-dword:00000001</pre>
<input type="checkbox"/>	<p>Replace all occurrences of <server> with the name of the WebFront server and <version> with the corresponding Lync/Skype version.</p> <p>2013 = 15.0 2016 = 16.0</p>
<input type="checkbox"/>	<p>Save the file</p>
<input type="checkbox"/>	<p>Import the registry file by clicking on it on all computers with Lync /Skype client installed that should have the integration enabled</p>
<input type="checkbox"/>	<p>Open a contact in Lync and click "... " then CTI for Service Manager to open the form and verify the functionality (see below)</p>  <p>The screenshot shows a contact's profile bar in Lync. At the bottom of the profile bar are three icons: a video camera, a telephone, and a computer monitor. To the right of these icons is a circular menu icon with three dots. A green arrow points from this icon to a context menu that is open. The menu contains the following items: 'Manage Recordings', 'IM Text Display Size' (with a right-pointing arrow), 'Change Font...', 'CTI for Service Manager 2012' (highlighted in blue), and 'Skype for Business Help'. Another green arrow points from the 'CTI for Service Manager 2012' item back to the profile bar area.</p>

Getting started with Command line integration

If you are not using Lync or Skype for Business and are looking to integrate a different call center application, you can absolutely do so using the command line integration option.

Prerequisites

- Call center agent application is able to execute a command line on an incoming call
- Call center agent application is able to pass the telephone number of the calling user as an argument in the command line being executed
- Phone number needs to be populated in CMDB to be able to match incoming call with user in CMDB

To enable computer telephony integration using command lines you need to configure the call center agent application to execute a command line as below:

Command line example

```
http://<webfrontServer>/webfront/CTI.aspx?PhoneNumber=%phoneNumber%
```

In the example above "<webFrontServer>" needs to be replaced with the name of your WebFront server or DNS alias. The "%phoneNumber%" needs to be modified differently based on which call center agent application you are using. Different products use different argument syntaxes.

When you have successfully configured the command line a browser window will open when the agent receives an incoming call. The URL of the browser window will contain the phone number which is passed to WebFront for processing.

Search options

By default, WebFront prepends a wildcard to the phone number when trying to locate a matching user in the CMDB of Service Manager. This means that if the phone number is e.g. a four-digit internal number you might end up matching too many users. As an example:

User A – Mobile number: "0702007722"

User B – Phone number: "7722"

When "User B" calls WebFront will find both User A and User B if you do not configure the command line to use exact match. To use exact match, you need to add "^" before the actual number argument.

For exact match, add "^"

```
http://<webfrontServer>/webfront/CTI.aspx?PhoneNumber=^%phoneNumber%
```

Special characters considerations

If the call center application forwards a number starting with a plus sign "+" this will be removed based on processing rules of a URL. Consider the users below when the following phone number is passed to WebFront: "+0702007722"

User A – Mobile number: "+0702007722"

User B – Phone number: "0702007722"

WebFront will find both user A and B (defined above) if the command line hasn't been built to use exact match (as described in the Search Options section). On the other hand, if the command line has been built to use exact match WebFront will only find user B since the plus sign is removed by the URL processing in web browsers and therefore isn't passed to WebFront. If your user objects in the CMDB has phone numbers registered with plus signs (or other special characters) and you want to do an exact match you will need to pre-process the phone number and replace the special character with its hexadecimal representation as described here: [https://technet.microsoft.com/en-us/library/aa226544\(v=sql.80\).aspx](https://technet.microsoft.com/en-us/library/aa226544(v=sql.80).aspx).

Example of exact match on phone number starting with a plus sign

```
http://<webfrontServer>/webfront/CTI.aspx?PhoneNumber=^%2B0702007722
```

Note: The command line above is showing a resulting command line where the argument sent by the call center application is "%2B0702007722". This mean the call center application has already replaced the plus sign with "%2B", which is the way it needs to be implemented for this to work.

Applying template based on argument

By default, no template is applied upfront when the CTI application is initialized unless a Default Template has been selected in the Settings tab. If you want to you can choose to pass a template id as an argument, this will initialize the CTI form using the specified template. Note, passing a template id as an argument will override the default template setting.

Using the template argument can be useful if your system is able to pre-qualify the call and pass different arguments based on the subject of the call.

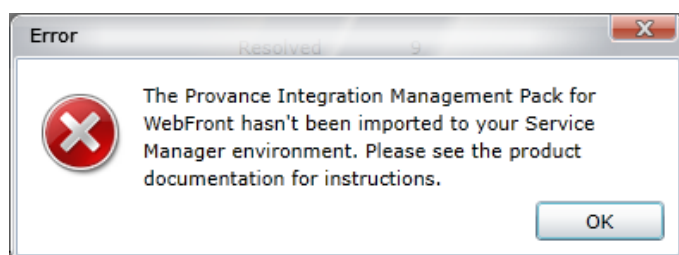
Example of template id as an argument:

```
http://<webfrontServer>/webfront/CTI.aspx?templateid=4cf10508-c474-94fd-55df-28cb7a6f3fb3
```

Note: It is the internal id of the template that you need to pass. This can be located using the Service Manager PowerShell Module.

Integration: Provance Asset Management

WebFront for Service Manager allows you to view information about Hardware Assets related to an Incident if you are using Provance Asset Management. To enable this, you need to have the Provance Asset Management 3.0 (or later) installed and import an integration pack that comes with WebFront for Service Manager. If the integration pack has not been imported, you will see the following dialog.



To import the integration pack for Provance Asset Management, follow the steps below.

On a server or client with Service Manager console installed	
<input type="checkbox"/>	Click Start – All Programs – Microsoft System Center – Service Manager – Service Manager Console
<input type="checkbox"/>	Click Administration tab
<input type="checkbox"/>	Select Management Packs
<input type="checkbox"/>	Click Import
<input type="checkbox"/>	Browse and select the following management pack: "C:\inetpub\wwwroot\WebFront\Bin\Gridpro.WebFront.IP.ProvanceAsset.Library.mpb" <i>Note: The path might differ if you have chosen to install WebFront beneath another WebSite</i>
<input type="checkbox"/>	Click Open
<input type="checkbox"/>	Click Import
<input type="checkbox"/>	Click OK to close the dialog

After importing the integration pack it is possible to use the console task called "View Related Hardware Assets" to view the asset information.

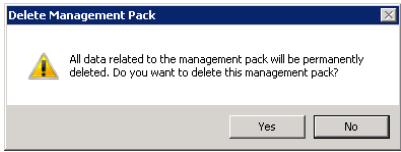
Uninstallation

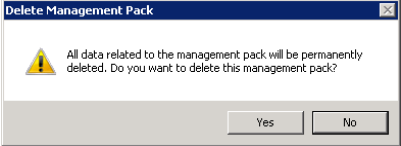
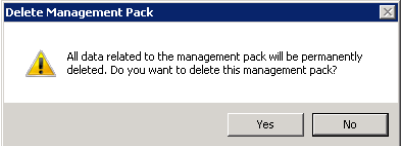
Software

Uninstalling WebFront is done by using the control panel applet.

On a server that has WebFront for Service Manager software installed	
<input type="checkbox"/>	Click Start – Control Panel
<input type="checkbox"/>	Click Uninstall a program
<input type="checkbox"/>	Right-click WebFront for Service Manager and select Uninstall
<input type="checkbox"/>	Click Yes
<input type="checkbox"/>	Click Yes , on User Access Control popup question
<input type="checkbox"/>	Uninstallation completed

Management Packs

On a server or client with Service Manager console installed	
IMPORTANT Management pack Gridpro.WebFront.ServiceManager.Presentation.Library contains the data model used to represent WebFront form customizations in the Service Manager database. After deleting this management pack your form customizations will be lost.	
<input type="checkbox"/>	Click Start – All Programs – Microsoft System Center – Service Manager – Service Manager Console
<input type="checkbox"/>	Click Administration tab
<input type="checkbox"/>	Select Management Packs
<input type="checkbox"/>	In center-pane select Gridpro.WebFront.ServiceManager.Library
<input type="checkbox"/>	Select Delete in right-pane
<input type="checkbox"/>	 Click Yes
<input type="checkbox"/>	In center-pane select Gridpro.WebFront.ServiceManager.Presentation.Library
<input type="checkbox"/>	Select Delete in right-pane

<input type="checkbox"/>	 <p>Click Yes</p>
<input type="checkbox"/>	<p>In center-pane select Gridpro WebFront ServiceManager IP ProvanceAsset Library</p>
<input type="checkbox"/>	<p>Select Delete in right-pane</p>
<input type="checkbox"/>	 <p>Click Yes</p>
	<p>Management Packs removal completed</p>