Request Management for Windows Azure Pack

Deployment Guide

Gridpro AB
Rev: 1.5.6954 (SCSM 2012 versions) & 2.0.6954 (SCSM 2016 & later)
Published: April 2019

Contents

Installation

The following sections will guide you through the basic installation steps required to start using Request Management for Windows Azure Pack. After completing the installation of the Admin- and Tenant Portal Extensions as well as the Request Management API you will need connect Windows Azure Pack to the Request Management API, see section "Connect Windows Azure Pack to the Request Management API".

NOTE: If your Windows Azure Pack deployment has been done through the Web Platform Installer, and if you did not de-select Request Management for Windows Azure Pack during the installation, you should already have the Admin- and Tenant Portal extensions of Request Management for Windows Azure Pack installed.

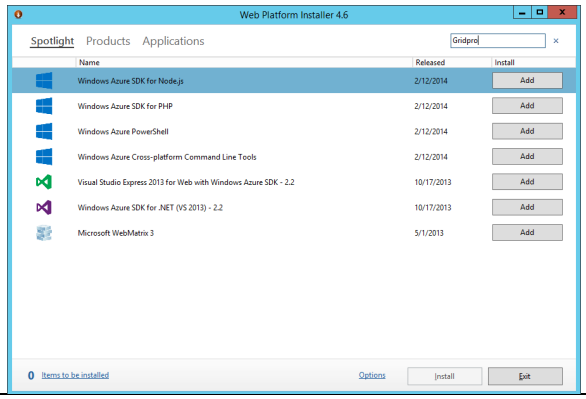
Admin Portal Extension

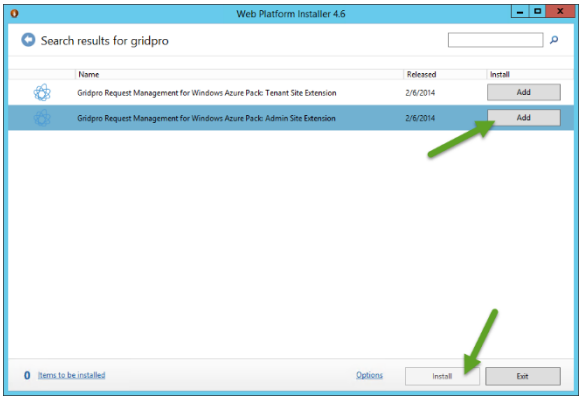
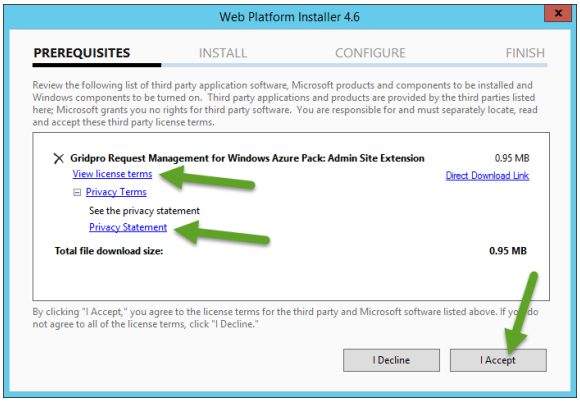
The following actions are required on each server hosting the Admin Portal (MgmtSvc-AdminSite) to install the Admin Portal extension of Request Management for Windows Azure Pack.

Prerequisites

This can only be installed on a web server running the Admin Portal of Windows Azure Pack. No additional requirements exist.

Installation Procedure

☐	**IMPORTANT:** Login using a user account that is a member of the local server administrator group
☐	Launch the **Web Platform Installer** (WebPI) *If the Web Platform Installer hasn't been installed already you can download it from here: http://go.microsoft.com/fwlink/?LinkId=255386*
☐	 In the top right search box, enter **Gridpro** and click Enter

☐		Select "**Gridpro Request Management for Windows Azure Pack: Admin Extension**" and click **Add** followed by **Install** to run the installation
☐		Review the **License- and Privacy Terms** and proceed by accepting thouse with the "**I Accept**" button
☐	Click **Finish** to complete the installation	

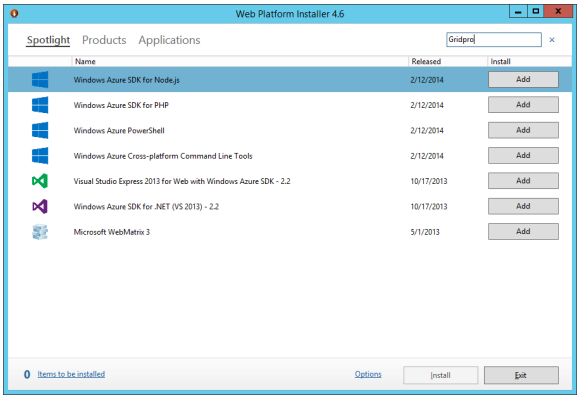
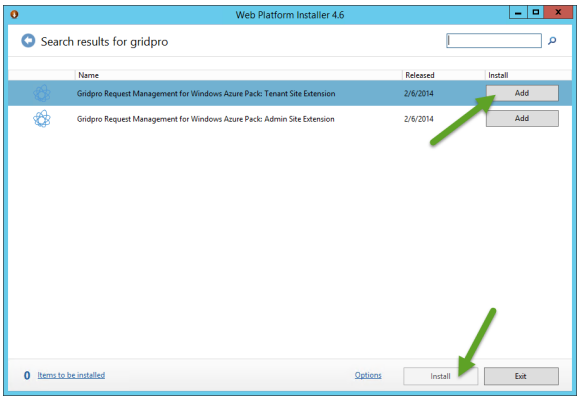
Tenant Portal Extension

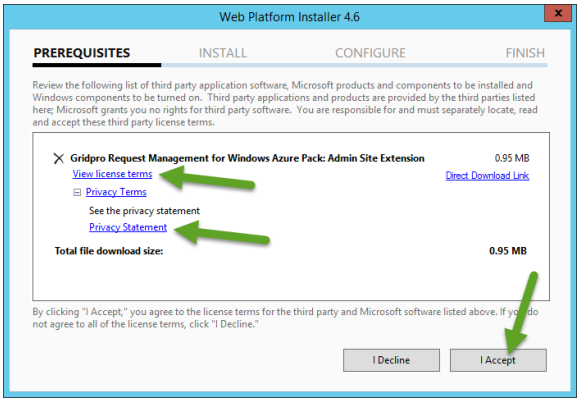
The following actions are required on each server hosting the Tenant Portal (MgmtSvc-TenantSite) to install the Tenant Portal extension of Request Management for Windows Azure Pack.

Prerequisites

This can only be installed on a web server running the Tenant Portal of Windows Azure Pack. No additional requirements exist.

Installation Procedure

☐	**IMPORTANT:** Login using a user account that is a member of the local server administrator group
☐	Launch the **Web Platform Installer** (WebPI) *If the Web Platform Installer has not been installed already, you can download it from here: http://go.microsoft.com/fwlink/?LinkId=255386*
☐	 In the top right search box, enter **Gridpro** and click Enter
☐	 Select the "**Gridpro Request Management for Windows Azure Pack: Tenant Extension**" entry and click **Add** followed by **Install** to proceed

☐	 Review the **License- and Privacy Terms** and proceed by accepting thouse with the "**I Accept**" button
☐	Click **Finish** to complete the installation

Request Management API

For each System Center Service Manager environment you want to connect you need to deploy an instance of the **Request Management API** web service.

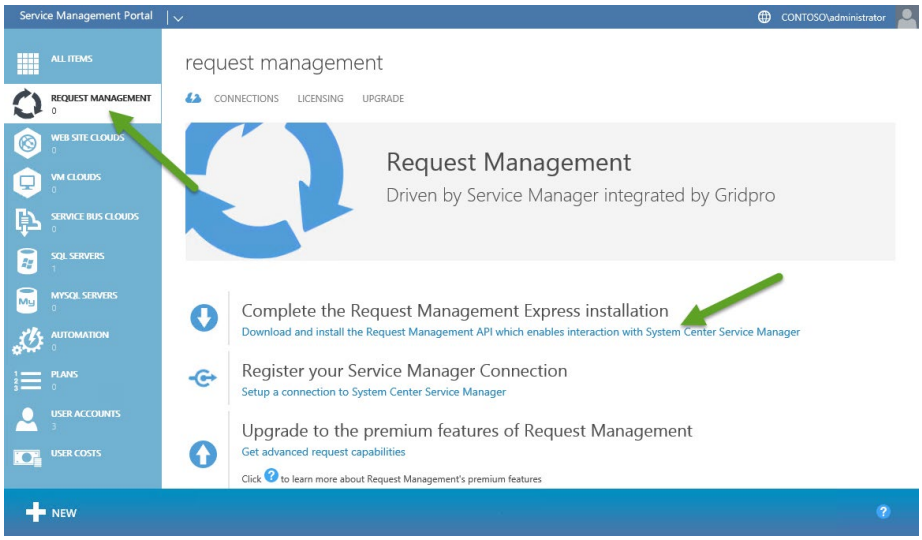
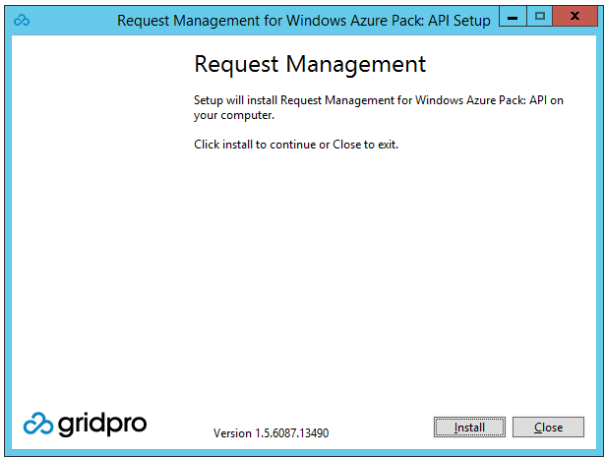
NOTE: The Request Management API needs to be installed in the same domain as the targeted System Center Service Manager is installed.

Prerequisites

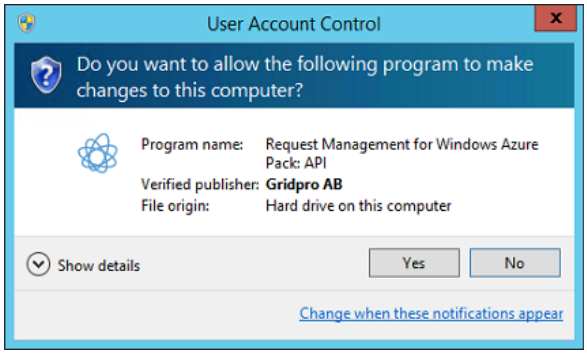
The following list shows the minimum prerequisites for the Request Management API.

- The server needs to be a Windows Server 2012 or later
- System Center 2012 Service Manager Console or later
- .Net Framework 4.5 or later
  The server needs have .Net Framework with the following features
  - .Net Framework 4.5 or later Features
    - ASP.NET 4.5 or later
- IIS (W3SVC)
  The server needs to be a web server with the following components
  - Web Server
    - Common HTTP Features
      - Default Document
      - Directory Browsing
      - HTTP Errors
      - Static Content
    - Health and Diagnostics
      - HTTP Logging
    - Performance
      - Static Content Compression
    - Security
      - Request Filtering
    - Application Development
      - ASP.NET 4.5 or later
      - ISAPI Extensions
      - ISAPI Filters
      - .Net Extensibility 4.5 or later

Installation Procedure

☐	IMPORTANT: The account used to run the installation needs to be: • Member of the local server administrator group • Administrator in the targeted Service Manager environment • Allowed to create stored procedures in the Service Manager database
☐	Login to the **Admin Portal** of Windows Azure Pack *Typically: https://<server>:30091/*
☐	 Click **Request Management** followed by the "**Download and install the Request Management API which enables interaction with System Center Service Manager**"
☐	Fill out the form as detailed as possible on the Gridpro web page and click Submit **NOTE:** Within a few minutes you will receive a download link for the **Request Management API.**
☐	On the server where you choose to install the **Request Management API**, run the downloaded file, **Request Management for WAP API vX.X.XXXX.exe**
☐	 Click **Install** to initiate the installation wizard

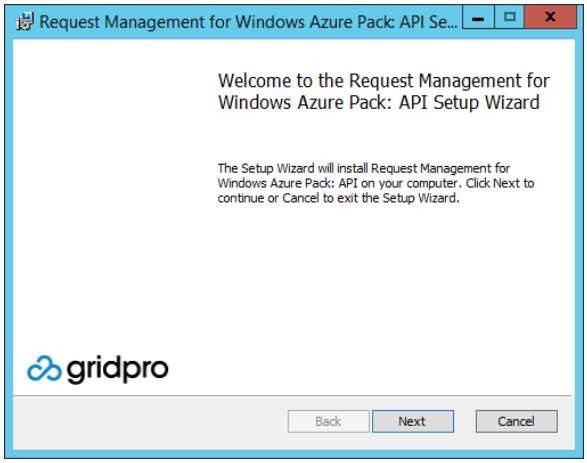
☐



Click **Yes** to allow the installation process to make changes to the computer

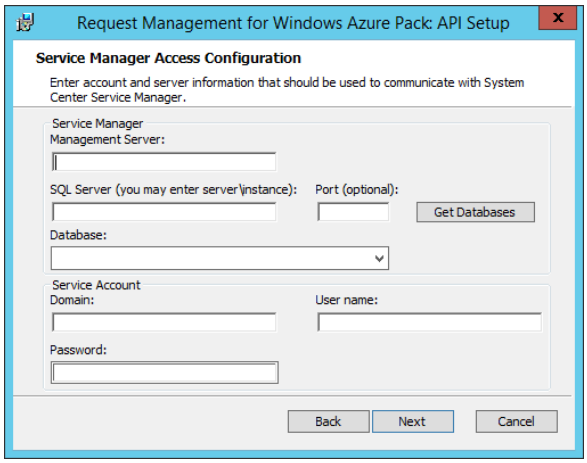
NOTE: This screen will not show under certain security settings, this is perfectly normal

☐



Click **Next** to start the installation

☐



Enter the name of the Service Manager server that you want the service to work against

Enter the name of the SQL server (and instance and port if not default) where the Service Manager database resides

Click "Get Databases"

Select the Service Manager database from the drop down list

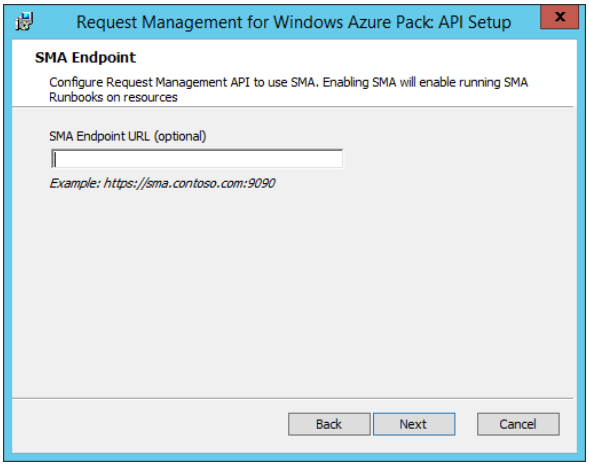
Enter credentials to use when communicating with Service Manager and SQL

NOTE: The account needs to be a Service Manager administrator and allowed to run a stored procedure in the Service Manager database. We recommend that you use the Service Manager Service Account to guarantee the required permissions.

Click **Next** to continue

When you click next some validation will take place which might take a few seconds to complete.

☐



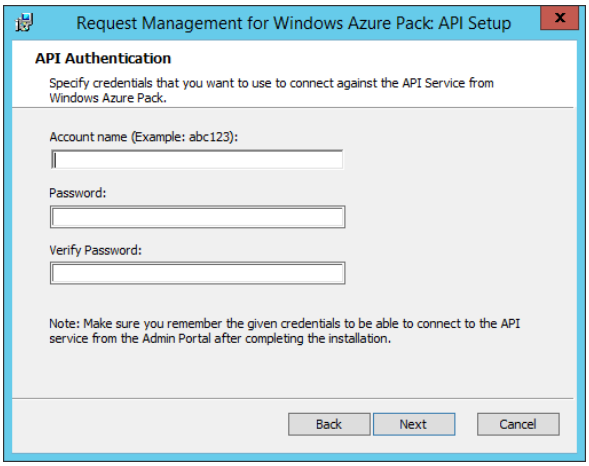
If you have an instance of Service Management Automation (SMA) running in your environment, add the url to the SMA WebService to enable executing runbooks from the Tenant Site

NOTE: This can be left blank in which case the feature will not be available. To enable it at a later time, see instructions in the appendix (Configuring Service Management Automation Integration).

NOTE: The Service Account specified in the previous screen needs to be member of the local security group called smaAdminGroup on the Service Management Automation server if you choose to use this feature.

Click **Next** to continue

☐

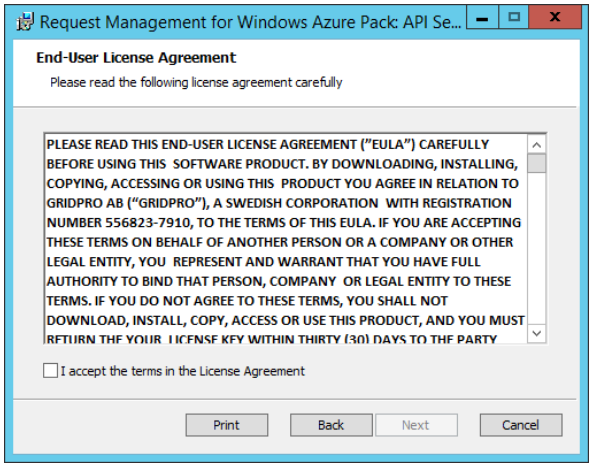


Enter an account name and password of your choice that you want to use when connecting to the service from the WAP Admin Portal

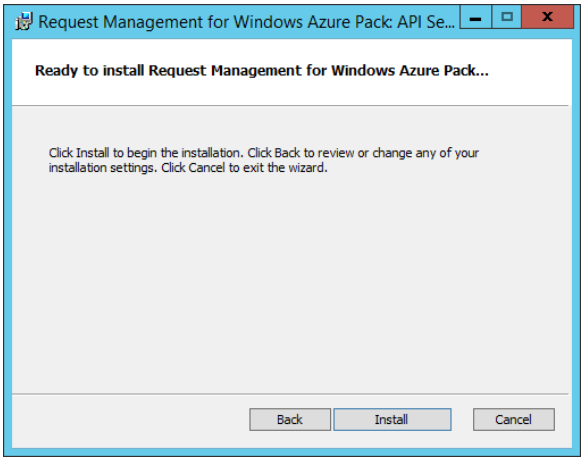
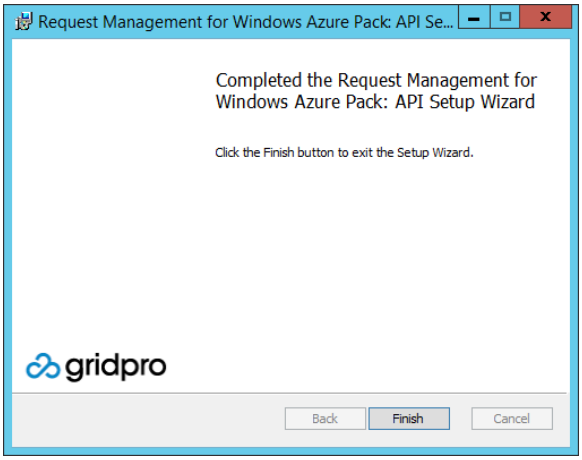
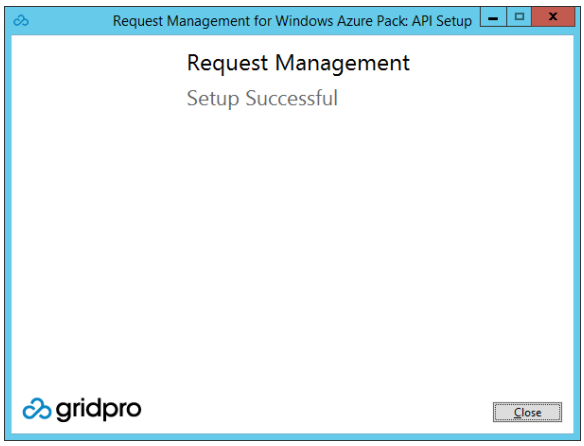
NOTE: Make sure you remember these values since they will be encrypted during the installation.

Click **Next** to continue

☐



Read Software License Agreement carefully and if you accept the terms check **I accept the terms in the License Agreement** then click **Next**

☐		Click **Install**
☐		Click **Finish** to complete the installation wizard
☐		Click **Close** to complete the installation

Update Request Management Admin/Tenant Sites

The Request Management for Windows Azure Pack: API download includes the Tenant- and Admin- Site Extension installers that are normally installed through the Web Platform Installer. These are updated more frequently than in the Web Platform Installer, you should therefore make sure you go through the steps in this chapter carefully.

This is to ensure you are running the latest versions of the Tenant- and Admin Site Extensions for Request Management for Windows Azure Pack.

Admin Site Extension Upgrade

Upgrade Procedure	
☐	Copy the download archive to the server(s) where you have the **Request Management for Windows Azure Pack: Admin Site Extension** installed
☐	Run the file **Gridpro.WAP.SCSM.AdminExtension.Setup.msi**
☐	Follow the wizard instructions to complete the upgrade
☐	Repeat the steps on all Admin Site servers if your setup includes multiple instances of these

Tenant Site Extension Upgrade

Upgrade Procedure	
☐	Copy the download archive to the server(s) where you have the **Request Management for Windows Azure Pack: Tenant Site Extension** installed
☐	Run the file **Gridpro.WAP.SCSM.TenantExtension.Setup.msi**
☐	Follow the wizard instructions to complete the upgrade
☐	Repeat the steps on all Tenant Site servers if your setup includes multiple instances of these

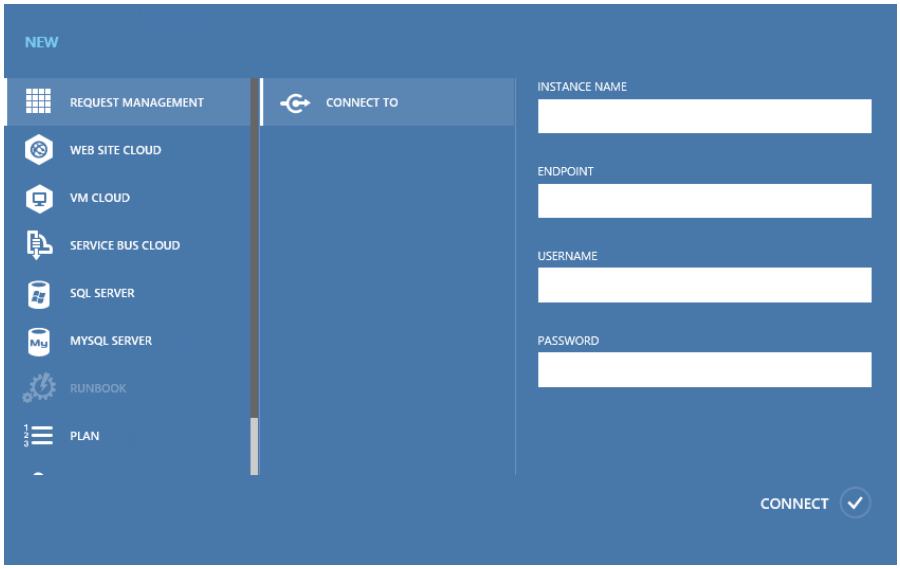
Post installation configuration

After installing Request Management for Windows Azure Pack, the following configuration is required before starting to use it on the Tenant Portal.

Connect Windows Azure Pack to the Request Management API

To start using Request Management for Windows Azure Pack you need to create your first connection to a Request Management API. Follow the steps below to create your first connection.

Configuration

☐	Go to **Windows Azure Pack Admin Portal**
☐	Click **Request Management**
☐	Click **Connections** tab
☐	Click **Add**
☐	Enter the following information. **Instance name:** Give the connection a name **Endpoint:** https://<apiservername>:30033 **Username:** *Username entered during installation of the Request Management API* **Password:** *Password entered during installation of the Request Management API* 
☐	Click **CONNECT** to complete and you can start using Request Management in Express mode

Upgrade

This section describes the procedure to upgrade Request Management for Windows Azure Pack from any previous version.

☐	As a best practice, start by updating the Windows Azure Pack components using Windows Update
To upgrade the Request Management for Windows Azure Pack: API *The web service that comes with Request Management for Windows Azure Pack*	
☐	If you haven't already received the latest download link from Gridpro, please contact sales@gridprosoftware.com to request a download link for the latest version of Request Management for Windows Azure Pack
☐	Download the current version of Request Management API
☐	Copy the download archive to the server(s) where you have the Request Management for Windows Azure Pack: API installed
☐	Extract the archive and run the file called: **Request Management for WAP API vX.X.XXXX.exe**
☐	Follow the wizard instructions to complete the upgrade **IMPORTANT:** If you are upgrading from version 1.3.9999 or earlier, please follow the below instructions to enable integration with Service Management Automation. 1. On each server where you have upgraded the Request Management API, edit the following configuration file: **"C:\inetpub\MgmtSvc-RequestManagementAPI\solidNonSensitiveSettings.config"** 2. Update the value of the setting called "OnPremiseAutomationUrl" as below (replace smaServerName your Service Management Automation server name): **<add key="OnPremiseAutomationUrl" value="https://smaServerName:9090/00000000-0000-0000-0000-000000000000" />** 3. Save and close the file More information see appendix: Configuring Service Management Automation Integration
To upgrade the Request Manangement for Windows Azure Pack: Admin Site Extension **IMPORTANT:** It is always mandatory to upgrade the Request Management Admin/Tenant Site at the same time as upgrading the Request Management API to keep versions in sync.	
☐	Copy the download archive to the server(s) where you have the **Request Management for Windows Azure Pack: Admin Site Extension** installed
☐	Run the file **Gridpro.WAP.SCSM.AdminExtension.Setup.msi**

☐	Follow the wizard instructions to complete the upgrade
To upgrade the Request Management for Windows Azure Pack: Tenant Site Extension **IMPORTANT:** It is always mandatory to upgrade the Request Management Admin/Tenant Site at the same time as upgrading the Request Management API to keep versions in sync.	
☐	Copy the download archive to the server(s) where you have the **Request Management for Windows Azure Pack: Tenant Site Extension** installed
☐	Run the file **Gridpro.WAP.SCSM.TenantExtension.Setup.msi**
IMPORTANT: You need to repeat the appropriate steps on all Tenant Site, Admin Site and Request Management API servers if your setup includes multiple instances of these.	

Appendix A

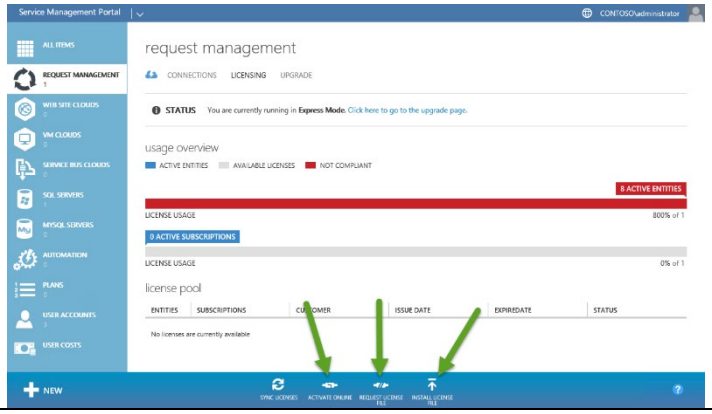
Upgrading to Premium Mode

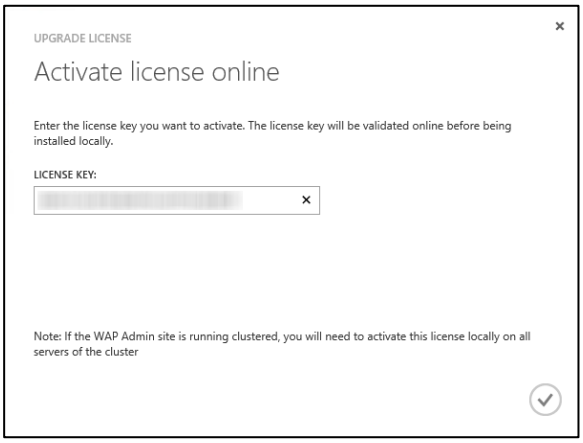
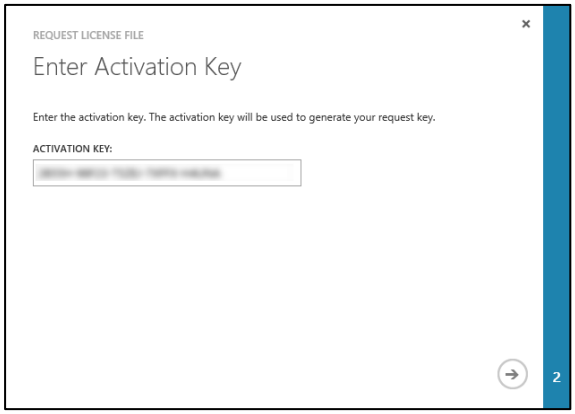
To take advantage of the full capabilities of the product you need to upgrade from Express to Premium mode.

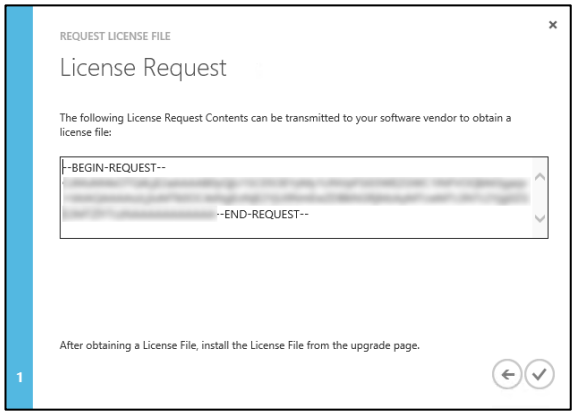
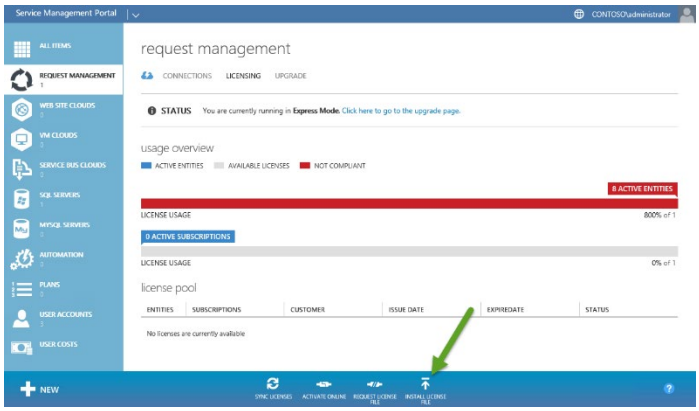
NOTE: If you have multiple Admin Portal servers sitting behind a load balancing cluster you need to follow the "Upgrade Procedure (multiple admin sites)".

To upgrade to Premium mode, follow these steps.

Upgrade Procedure (single admin portal server)

☐	If you haven't already received a license key from Gridpro, please contact sales@gridprosoftware.com to purchase a retail key or request an evaluation key.
☐	Go to **Windows Azure Pack Admin Portal**
☐	Click **Request Management**
☐	 Click **Licensing** tab

	<u>If you have Internet access</u>
☐	Click **Activate Online**
☐	 Enter the license key and click the Activate button in the lower right corner
☐	Done
	<u>If you don't have internet access</u>
☐	Click **Request license file**
☐	 Enter license key and click the **arrow** in the lower right corner

☐	 Copy the request data in the textbox
☐	Send the information to support@gridprosoftware.com to request a license activation. Back in the Request License File dialog, click the **checkmark** to close the wizard.
After receiving a license file from support@gridprosoftware.com:	
☐	 Click **Install license file**
☐	Select the license file
☐	Click the **checkmark** in the lower right corner
☐	Done
To validate that the license has been installed, see “Licensing status”	

Upgrade Procedure (multiple admin portal servers)

☐	If you haven't already received a license key from Gridpro, please contact sales@gridprosoftware.com to purchase retail- or request an evaluation key. Remember to state your number of admin portal servers.
You need to repeat the following steps on each Admin Portal server	
☐	Login in locally on the Admin Portal server
☐	Start a command prompt
☐	Execute the following command: `cd "C:\inetpub\MgmtSvc-AdminSite\bin"` NOTE: If your admin site has a custom path, please adjust to that path.
<u>If you have Internet access</u>	
☐	Execute the following command: `RMLicenseActivation /a <your license key>` Where the "<your license key>" should be replaced with the license key provided by Gridpro
☐	Done
<u>If you don't have internet access</u>	
☐	Execute the following command: `RMLicenseActivation /g <your license key>` Where the "<your license key>" should be replaced with the license key provided by Gridpro
☐	Copy the output and send the information to support@gridprosoftware.com to request a license activation
After receiving a license file from support@gridprosoftware.com	
☐	Execute the following command: `RMLicenseActivation /o <path to license file>` Where the "<path to license file>" should be replaced with the path to the license file provided by Gridpro
☐	Done
To validate that the license has been installed, see "Licensing status"	

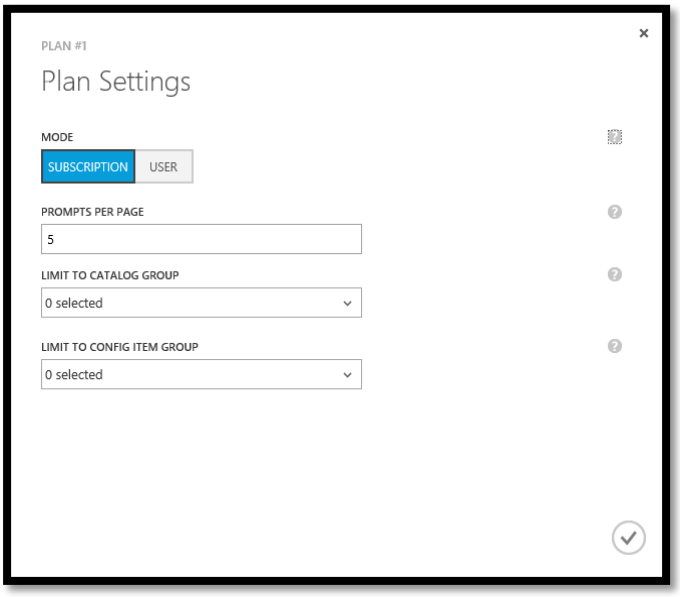
Plan Settings

Each plan that includes the Request Management service can be configured in a number of ways to cover a large number of different scenarios. In the image below you can see the different options available on a plan.

- Mode
  - Subscription: Every user that has access to the subscription will be able to associate a request with the subscription and will be able to see all tickets associated with the subscription in the Requests view.
    Note: This is what you want to use to allow users to "share" tickets.
  - User: Every user that has access to the subscription will be able to associate a request with the subscription. However, a user will only be able to see the requests where he/she is the "affected user".
    Note: Each time a request is created in System Center Service Manager from Windows Azure Pack, the user logged into WAP will be stated as the "affected user" automatically.
- Prompts Per Page: Decides how many questions should be rendered per page in the "New Request Wizard" which renders based on the configuration in the service catalog in Service Manager. In the case of a query result prompt being used in an offering, the query result prompt will be rendered on a separate page to avoid scrolling.
- Limit to Catalog Item Group: Choose which Catalog Item Groups, defined in System Center Service Manager, to use to limit the access to the offerings in the Service Catalog in SCSM.

IMPORTANT: A Request Offering will not be visible to a user unless the user has access to both the Request Offering and the Service Offering(s) it is linked to.

- Limit to Config Item Group: Choose which Groups, defined in SCSM, to use to limit the access to configuration items in Service Manager for a subscription associated to the plan.



File upload – Required Configuration

If you want to use the possibility to upload files in forms defined by the Service Catalog in System Center Service Manager, you need to configure Windows Azure Pack to allow sending larger data volumes than normal since the default values only allows you to send files up to 30 kilobytes.

To increase the maximum limits for data being sent through the Windows Azure Pack Tenant Portal, go to one of your servers hosting the Tenant Portal and follow these steps.

1. Open a PowerShell command prompt as Administrator
2. Enter the following commands:

```
cd "C:\Program Files\Gridpro\Request Management for Windows Azure Pack\Tools"
.\Set-MaxUploadSize.ps1
```

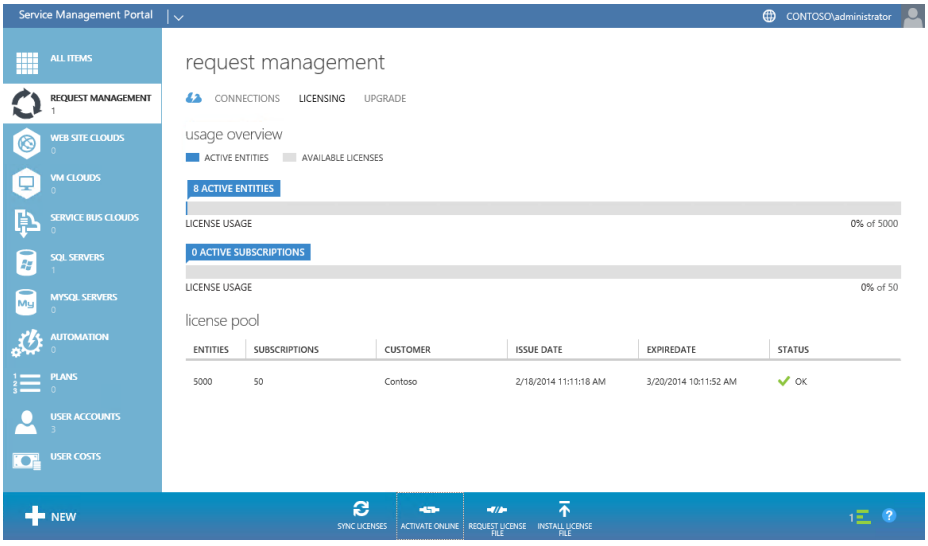
3. After passing the prerequisites check, you are asked to specify the number of megabytes you want to allow being sent through Windows Azure Pack. Enter the preferred limit and press **Enter**.
4. After successfully completing the script, repeat the procedure on all servers running one of the following web sites:
    a. MgmtSvc-TenantSite (Tenant Site)
    b. MgmtSvc-TenantAPI (Tenant API)

NOTE: The script is only available on the servers running the Tenant Site, you need to copy the script to server running the Tenant API.

Licensing Status

To review your current licensing status, go to the Admin Portal and follow these steps.

1. Click **Request Management**
2. Click **License**



In the license pool you can see all installed licenses, their expiry date and the number of entities they are valid for. The status on each license is just referring to the expiry date of the license.

The usage overview shows you the amount of measured entities in your environment compared to the number of entities you are licensed for.

NOTE: If the amount of measured entities goes above the number of entities you are licensed for a message will be displayed on the portal and you will be violating the license agreement.

Locating existing users in the CMDB

When a user is logged into the Tenant Portal the Request Management will try to locate that user in a number of scenarios:

- When loading current requests (when plan service settings is in "User" mode)
- When loading current activities
- When creating a new request

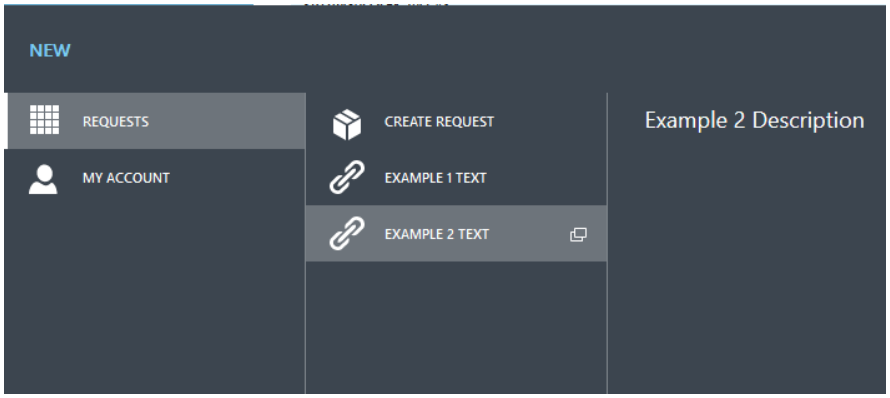
To locate the user object in the CMDB the login name of a user is used to search against user principal names (UPN) in the CMDB. If a user isn't found when retrieving current requests or activities, this is treated as a perfectly valid scenario and no errors or warnings will be displayed. However, if a user is not located at the time of creating a new request a new user object will automatically be created in the CMDB.

NOTE: If you wish to disable the creation of users automatically you can do so by editing the file called **solidNonSensitiveSettings.config** on the Request Management API Site and set the key called **CreateNewUserAutomaticallyInSCSM** to **false**.

Configuring Custom Links

In Request Management for Windows Azure Pack it is possible to add custom links to the Create Menu in the bottom part of the page. The links are highly configurable with properties like text, icon and description.

An example of custom links:



Adding Links

The custom links are configured on the server hosting the Tenant Site. If multiple servers are used (e.g. load balancing), these changes have to be made to all servers.

1. Open the file Customization.js located under:
   <TenantSite-InstallDir>\Content\ServiceManagerTenant\Scripts\Customizations\
   Typically: C:\inetpub\MgmtSvc-TenantSite\Content\ServiceManagerTenant\Scripts\Customizations
2. By default, the file contains two disabled examples of links, enabled them by removing the leading "//" them so that the file looks like:

```
(function ($, global) {
    "use strict";

    function getExternalLinks() {
        return [
            {
                Text: "Example 1 Text",
                Description: "Example 1 Description",
                Url: "http://www.example1.com",
                OpenInNewWindow: true,
                Icon: "Link"
            },
            {
                Text: "Example 2 Text",
                Description: "Example 2 Description",
                Url: "http://www.example2.com",
                OpenInNewWindow: false,
                Icon: "Link"
            }
        ];


    }

    global.ServiceManagerTenantExtension = global.ServiceManagerTenantExtension || {};
    global.ServiceManagerTenantExtension.Customizations = {
        getExternalLinks: getExternalLinks
    };
})(jQuery, this);
```

3. This will add two links to the menu. Each link can be customized with:
   - Text – The link text
   - Description – The description will be shown to the right of the link when selected
   - Url – The Url to open when clicked
   - OpenInNewWindow – If set to true, the link will be opened in a new window/tab, if set to false, it will open in the same window/tab.
   - Icon – An icon to the left of the link text (All available icons are described in the Icon section)
4. To add more links, simply add a new block like:

```
{
    Text: "Example 2 Text",
    Description: "Example 2 Description",
    Url: "http://www.example2.com",
    OpenInNewWindow: false,
    Icon: "Link"
}
```

   Note: The blocks should be separated by "," like the example
5. After saving the file, run iisreset from a command prompt on the server(s) hosting the tenant site for the changes to take effect.

Icons

There is a set of predefined icons that can be used with the link. To set the icon, the Icon property of the link should be set to the corresponding label from the table below.

	HostedService
	WebSite
	SystemCenterExtension
	StorageAccount
	NetworkExtension
	Database
	QuickCreate
	FromMarketplace
	AddSubscription
	AccountsAdminMenuItem
	NotificationAdminMenuItem
	PlansAdminMenuItem
	WebSystemAdminMenuItem
	SystemCenterAdminExtension
	MySqlAdminMenuItem
	SqlAdminMenuItem
	MediaService
	ConnectTo
	MobileService
	Data
	AppServices
	Network
	Compute
	Import
	FromNetcfg

	Store
	ServiceBusTopic
	ServiceBusQueue
	ServiceBusRelay
	RegisterDNS
	ActiveDirectoryACS
	ServiceBusNotificationTopic
	WebDomain
	RegisterLocalNetwork
	ReportingServices
	HDInsightExtension
	RecoveryServices
	ServiceBus
	BizTalk
	AutomationAdminExtension
	VirtualMachineRoleExtension
	TrafficManager
	Cdn
	VisualStudio
	Link
	GameServices
	XboxLiveCompute
	GameCompute
	Addons
	Caching

Configuring Service Management Automation Integration

This section contains useful information on how to setup the communication between Request Management for Windows Azure Pack and Service Management Automation (SMA) to enable SMA runbooks to be executed from the Tenant site in Windows Azure Pack.

Endpoint Address

The communication to SMA is performed through the Request Management API by using the address stated in the parameter called "**OnPremiseAutomationUrl**" (see yellow mark in the table below) which can be found in the file called **solidNonSensitiveSettings.config** on the server(s) where the Request Management API is installed. Normally the file has the following location:
C:\inetpub\MgmtSvc-RequestManagementAPI\solidNonSensitiveSettings.config

```
<?xml version="1.0" encoding="utf-8"?>
<!--
Appsettings and ConnectionStrings configuration is separated from web.config to retain settings during upgrade
 -->
<nonSensitiveSettings>
 <add key="SMServer" value="sm3.gridpro.se"/>
 <add key="CreateNewUserAutomaticallyInSCSM" value="true"/>
 <add key="ScriptPath" value="c:\Scripts\"/>
 <add key="OnPremiseAutomationUrl" value="https://sma.contoso.com:9090/00000000-0000-0000-0000-000000000000"/>
 <add key="IgnoreCertificateValidationForAutomation" value="true"/>
</nonSensitiveSettings>
```

If you have upgrade from a version lower than 1.3.9999, or left the value blank during the initial installation, the url needs to be configured manually. To set the address manually, enter the address to your SMA web service (normally on port 9090) and add "/00000000-0000-0000-0000-000000000000" after the address as the value of **OnPremiseAutomationUrl** in the config file.

NOTE: If you have a load balanced environment, don't forget to update the setting on all servers running the **Request Management API**.

Hardening Security for Production Environment

Before moving into a production environment you should make sure you follow these instructions to secure the communications of Request Management for Windows Azure Pack.

Securing the Request Management API web service

During installation of the Request Management API a self-signed certificate is used to setup the binding for the web service (MgmtSvc-RequestManagementAPI). You should replace this certificate with a trusted certificate to make sure you secure communications between Windows Azure Pack and the Request Management API (MgmtSvc-RequestManagementAPI).

Securing communication to Service Management Automation

If Request Management for Windows Azure Pack has been setup to communicate directly to Service Management Automation (see section Configuring Service Management Automation Integration in this appendix) you should make sure you have a trusted certificate on the SMA web service and configure the Request Management API to not allow communications with endpoints using an untrusted certificate. To instruct the Request Management API to not communicate with SMA if SMA is using an untrusted certificate you need to change the value of the parameter called **IgnoreCertificateValidationForAutomation** to **false** (see yellow marking in the table below) in the configuration file called **solidNonSensitiveSettings.config** on the server(s) where the Request Management API is installed.

```
<?xml version="1.0" encoding="utf-8"?>
<!--
Appsettings and ConnectionStrings configuration is separated from web.config to retain settings during upgrade
 -->
<nonSensitiveSettings>
 <add key="SMServer" value="sm3.gridpro.se"/>
 <add key="CreateNewUserAutomaticallyInSCSM" value="true"/>
 <add key="ScriptPath" value="c:\Scripts\"/>
 <add key="OnPremiseAutomationUrl"
value="https://sma.contoso.com:9090/00000000-0000-0000-0000-000000000000"/>
 <add key="IgnoreCertificateValidationForAutomation" value="false"/>
</nonSensitiveSettings>
```

Tips and Tricks

This section contains useful tips and tricks for Request Management for Windows Azure Pack.

Published state "WAP"

There is now a custom published status for request offerings called WAP. Setting the custom published status on an offering will:

- Make the offering only appearing in WAP, it would not appear in the OOB SSP that comes with Service Manager
- Make it possible to skip mapping prompt answers to properties on the targeted work item
  Note: Make sure you have completed the prompt configuration before exposing the offering to your users

Published state "WAP: Action Type"

In addition to the "WAP" status, there is a published status called "WAP: Action Type". A Request Offering with this status will not show in the Create Request Wizard, but will still be available for use with Request Actions. See the chapter Action Configuration in the Operations Guide for more information on how to configure Actions.

Support for Change Requests

Request Management for Windows Azure Pack adds support for adding Change Request offerings in the Service Catalogue, these however should only be published to WAP and never to the out-of-the-box (OOB) Self Service Portal that comes with Service Manager. The OOB portal will fail on submit with such an offering.

Known Limitations

This section describes known issues with this version of the product.

- Request Offering: "DisplayOnly" mode is only supported for Query Result-, Text-, Integer-, List-, and Decimal Prompts, all other prompt types are ignored in DisplayOnly mode
- Request Offering: Unbound MPEnumeration lists will cause the request wizard to fail
  Note: This can only happen when using the "WAP" publish alternative since this disables all validation normally done when using the standard "Published" status
- Usage: When running in "User" mode the usage data is displayed per subscription
- Query Result Prompt: Advanced criteria using "Generic Properties" cannot be used in combination with "Limit to Config Item Group" functionality

Abbreviation

SSP – Self Service Portal
OOB – Out-of-the-box