Quest

Metalogix® StoragePoint 5.8

Atmos Adapter Guide

Quest Software Inc.
Attn: LEGAL Dept.
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Metalogix® StoragePoint
Updated March 2019
Version 5.8

Contents

1

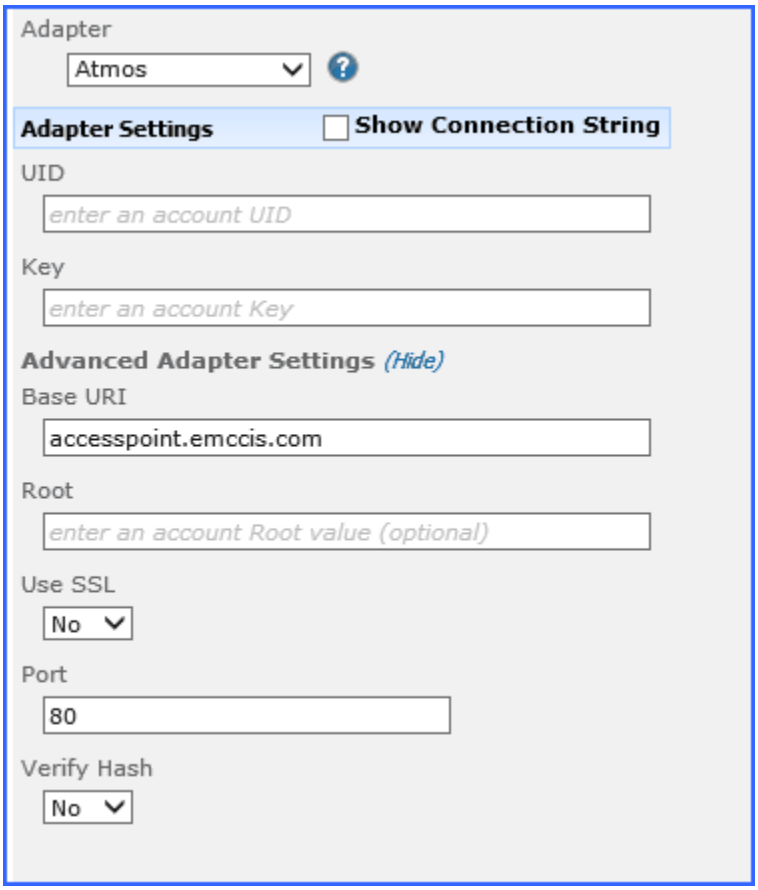
Atmos Adapter Configuration

This section will provide you details on how to configure a storage endpoint's connection string to utilize the Atmos Adapter. Please refer to the StoragePoint Refernece Guide for information on managing Storage Endpoints.

On the Application Management page, click *Storage and Backup Endpoints*.

Click *Create New Endpoint* or click the name of an existing storage endpoint that you want to edit.

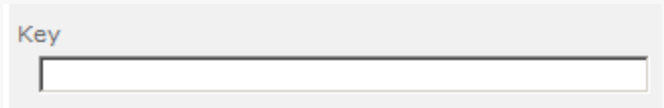
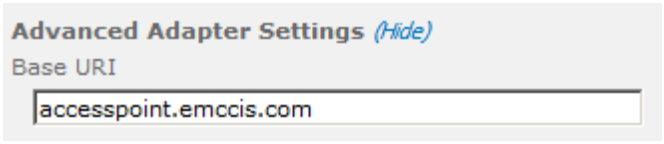
Click the *Show* link next to the Advanced Adapter Settings to see the additional fields.



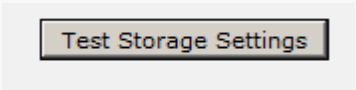
Atmos Adapter Connection String Parameters

Setting	Value/Options
Name	Enter the unique name of the

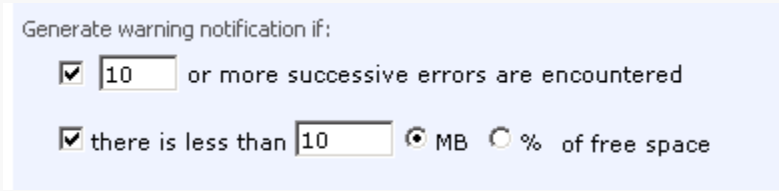
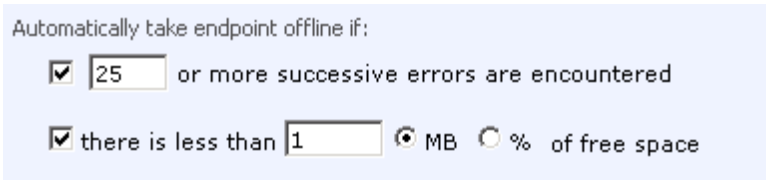
Setting	Value/Options
	Storage or Backup Endpoint.
Type  See Backup Services Settings in the Reference Guide for more information on how Backup Endpoints are used.	*Primary* – this endpoint will be available for externalization when creating storage profiles. *Backup* – this endpoint will be in the Backup Services dropdown on the profile page. The selection is locked down when saving.
Status  	*Online* – Storage Endpoint should be available to associate to a Storage Profile and accept BLOBs. (default) *Offline (Read Only)* – A storage endpoint can be configured, but not made available for externalizing content. The BLOBs already on the endpoint are still read only.

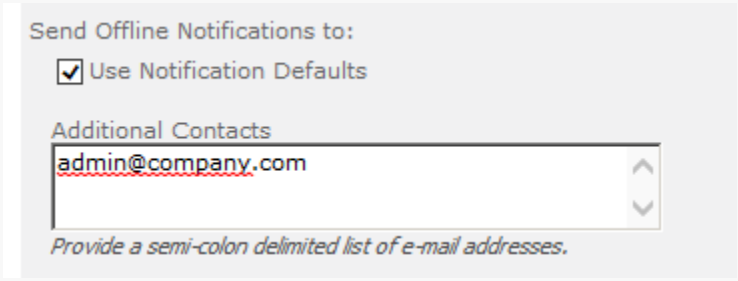
Setting	Value/Options
	Select the adapter for the endpoint that is being created.
	The username to use when connecting to the server. This is equivalent to the Token ID provided with your Atmos online account.
	The base64 encoded shared secret to use when signing requests to the server.
	IP address or host name that represents the Atmos instance or specific node to be used. Default = accesspoint.emccis.com.
	The starting folder/container within your Atmos namespace under which all folders and files will be created.

Setting	Value/Options
	(*yes/no*) Determines whether or not the adapter negotiates an SSL connection for all data (and metadata) transfers. See Appendix A for details on adding a trust relationship. Default = No.
	The port on the server to communicate with. Default = 80 (443 if UseSSL is Yes).
	(*yes/no*) Includes a check-sum operation after each blob transfer. Allows the adapter to detect and log data integrity errors immediately. Default = No.
	If the endpoint is on a WORM (Write Once, Read Many) device, Unused BLOB Cleanup

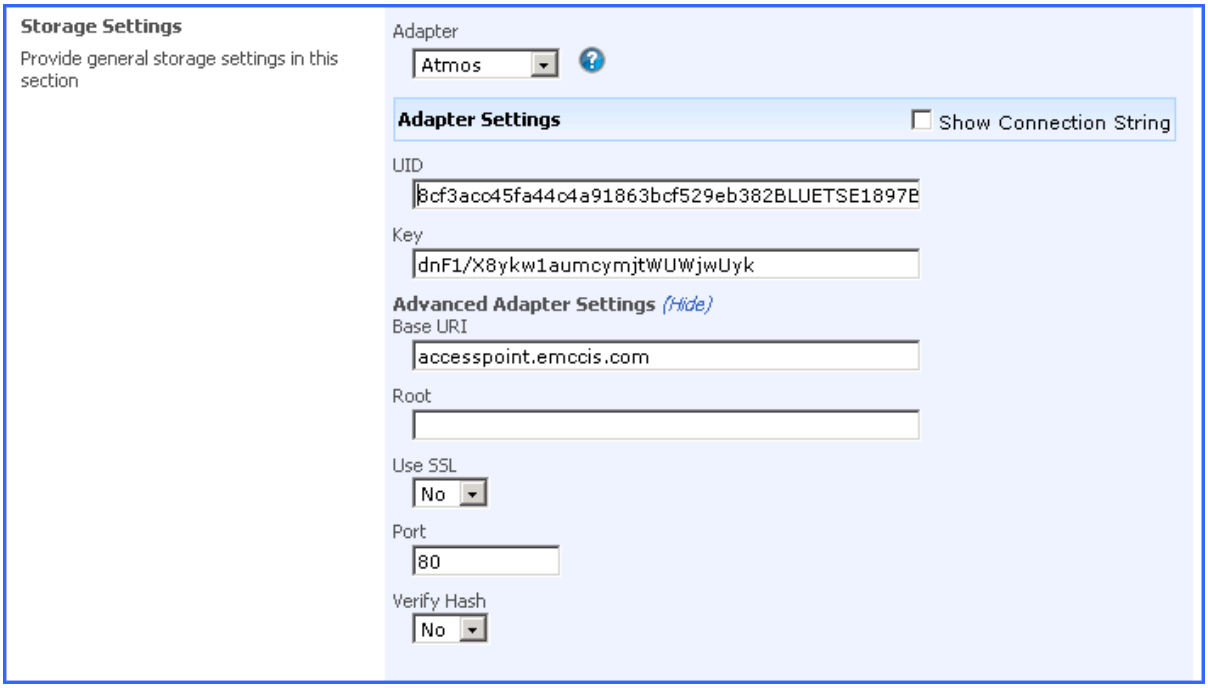
Setting	Value/Options
	will ignore this endpoint.
	*No* – Externalized content BLOBs are not placed in folders. *Yes* – Externalized content BLOBs are placed in folders (default). If *Folder Content in BLOB Store* is *Yes* then you can select a date/time folder scheme from the dropdown. YYYY/MM/DD/HH/MM is the default.
	The Test Storage Settings button can be used at this point, or after completing the endpoint configuration, to verify that the endpoint is accessible. For some adapters, testing the connection will create the folder

Setting	Value/Options
	if it doesn't already exist.
Compress Content in BLOB Store No *Content is compressed using the GZip/Deflate method.*	*No* – Externalized content BLOBs are not compressed (default). *Yes* – Externalized content BLOBs are compressed.
Encryption Method for Content in BLOB Store None	*None* – Encryption will not be applied to externalized BLOBs (default). *AES (128 bit)* – 128 bit AES encryption will be applied to externalized BLOBs. *AES (256 bit)* – 256 bit AES encryption will be applied to externalized BLOBs.
Encryption Key Passphrase Generate Key *Enter a passphrase to be used to generate a key or leave blank to generate a random key. The pass phrase entered is **not** saved with the Endpoint.*	Enter a passphrase to use when generating the encryption key. Using a

Setting	Value/Options
	passphrase will help you re-create the encryption key if necessary. You can generate a random key by leaving the box blank and clicking the *Generate Key* button. The encryption key passphrase will be hidden.
	A warning email can be sent if it encounters errors.
	An online storage endpoint can be automatically taken offline if it encounters errors. If a storage endpoint is taken offline automatically, BLOBs that were intended to be written to that endpoint will go to the content database.

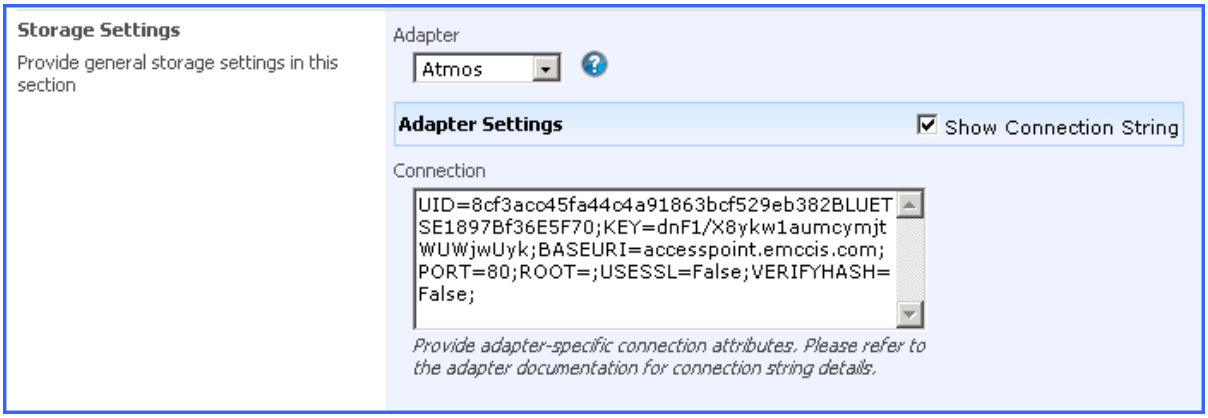
Setting	Value/Options
	Default email addresses for system error and offline notification can be entered. Check the box to include the list of Default Notification Contacts specified on the General Settings page.

Example Storage Endpoint using Atmos Adapter



Click the *Show Connection String* checkbox to edit the connection string. Otherwise, fill in the connection fields shown for the adapter selected. Notice that the connection string parameters are name/value pairs separated by semi-colons when editing using the Show Connection String

option.



NOTE: Adapter parameters are not case-sensitive.

NOTE: You should always use a passphrase when generating encryption keys. The passphrase gives you a means of re-creating keys should they become unrecoverable or corrupt. It is very important to remember or record the passphrase outside of Metalogix StoragePoint. Otherwise, encrypted content could become irretrievable in the event of a database failure.

If you choose to externalize content you should test the storage profile settings by clicking the *Test Storage Settings* button. A message under the button will indicate whether or not the test was successful. If the test fails the message will include the error that was the root cause of the failure.

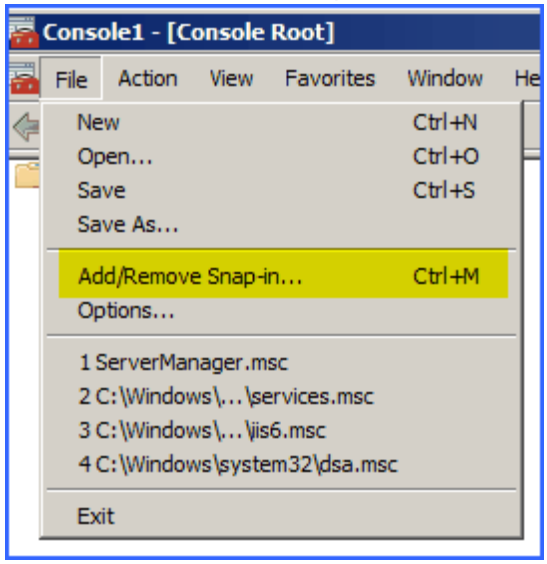
NOTE: When testing access to an endpoint from within Central Administration, the Identity of the Application Pool hosting the Central Administration Site is the one that is being used for the test. If there are different Identities used for other Web Applications in the Farm then those identities will also need access but cannot be tested from within Central Admin itself. See BLOB Store Security and Metalogix StoragePoint Required Privileges in the Metalogix StoragePoint Reference Guide.

Appendix: Using SSL with EMC Atmos

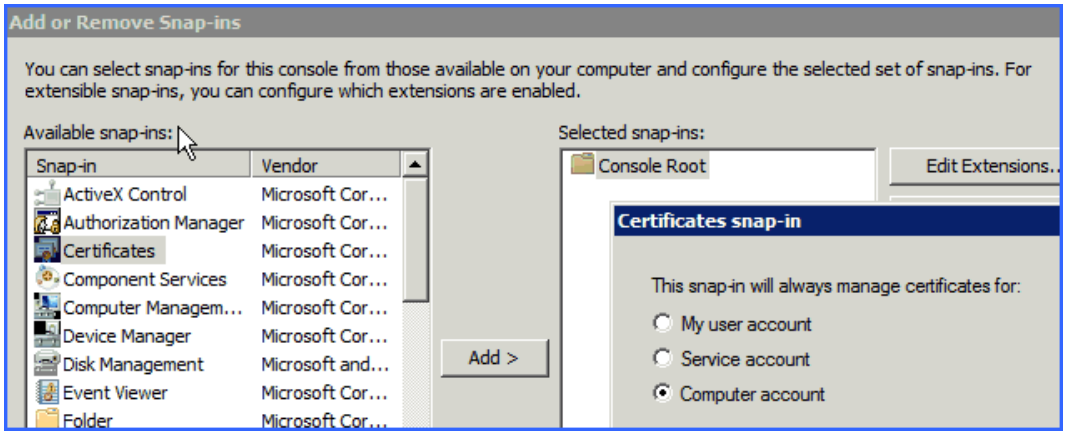
In order for the StoragePoint EMC Atmos adapter to use SSL to communicate with Atmos, the Atmos instance's certificate must be added to the SharePoint certificate store. The following steps describe how to do this:

1. Click Start->Run. Enter 'mmc.exe' and press Enter.

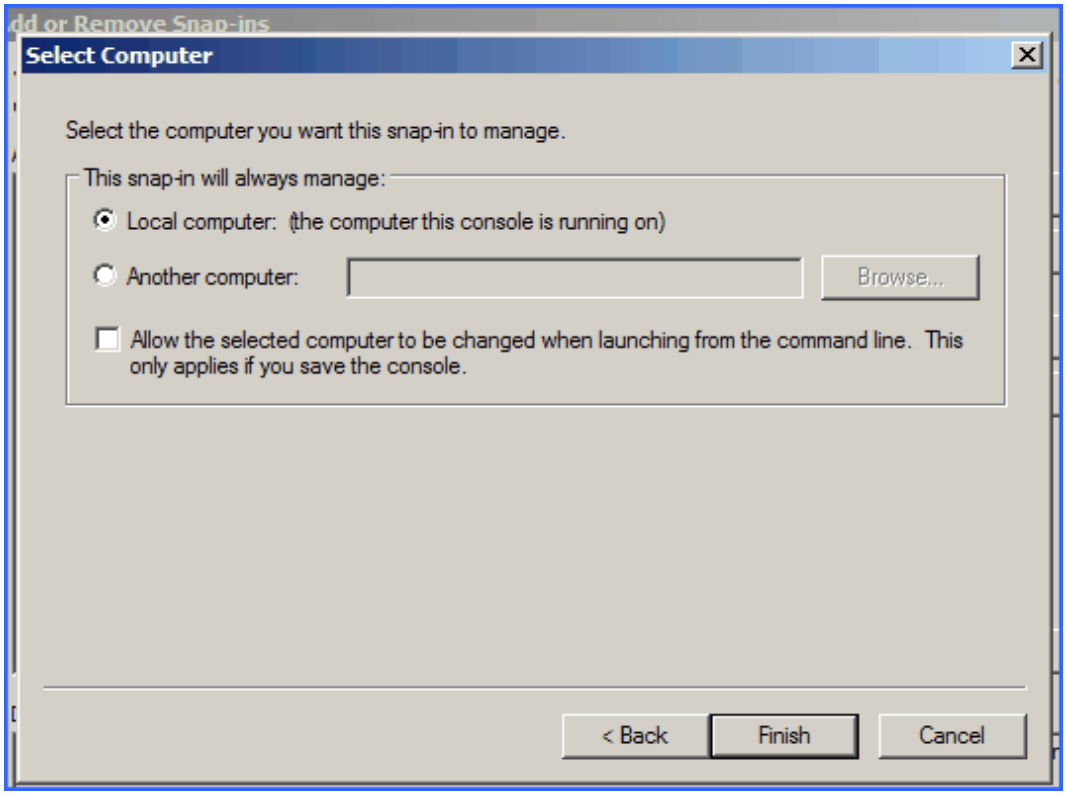
2. On the File menu, click Add/Remove Snap-In.



3. Click Certificates on the left, then click Add. A new window opens; select Computer Account and click Next.

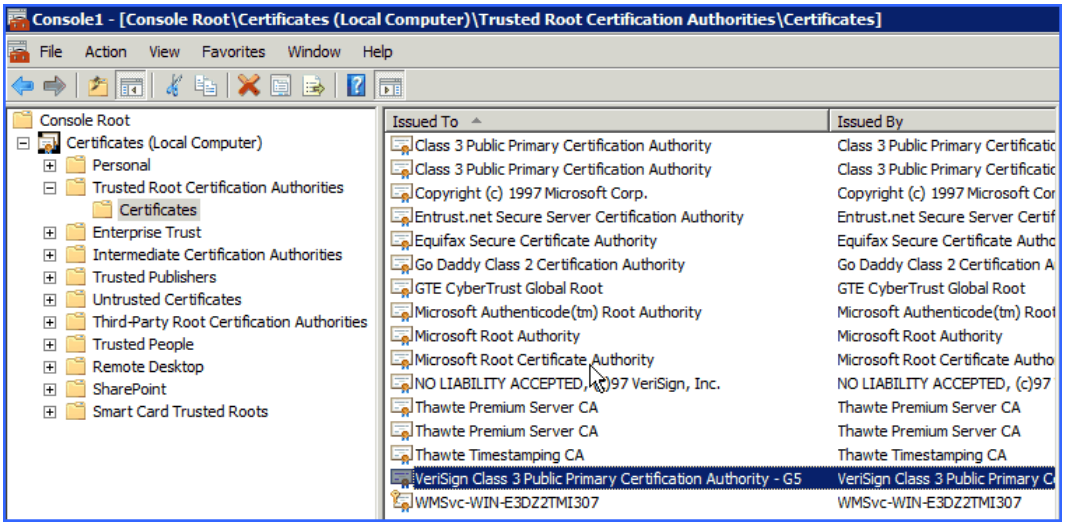


4. Select Local Computer and click Finish.

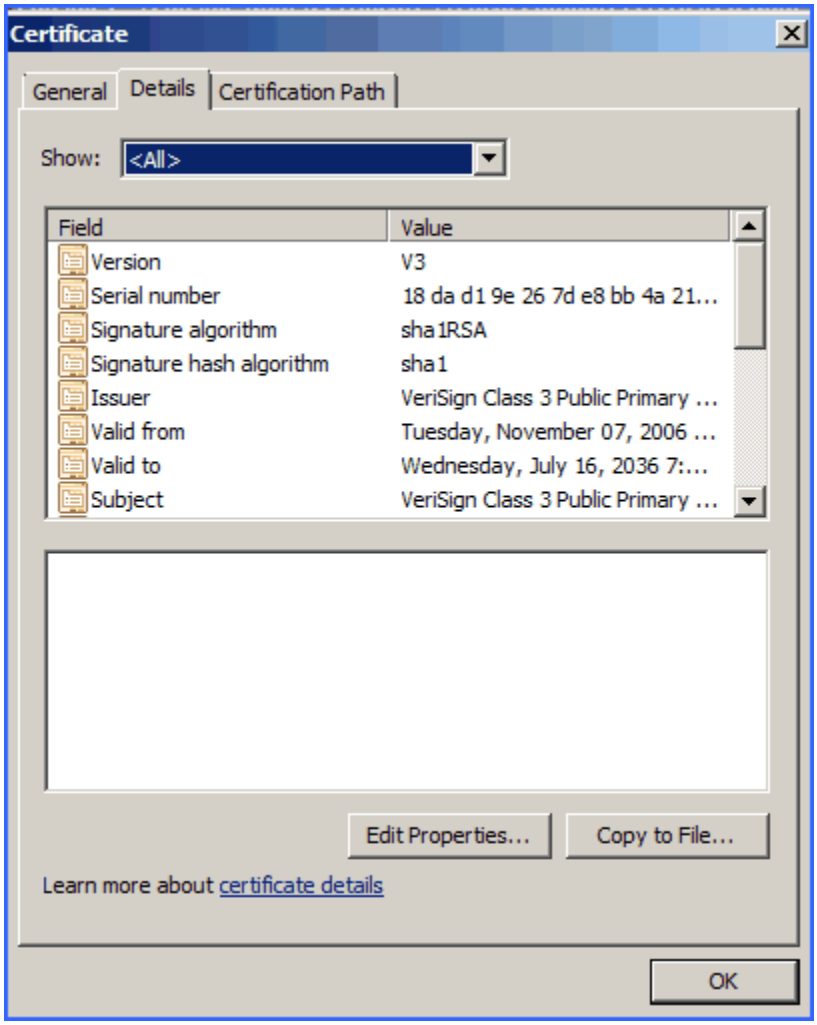


5. Click OK.

6. Expand Certificates (Local Computer)->Trusted Root Certification Authorities->Certificates. Find the root certificate. For AT&T this is the Verisign "G5" certificate:



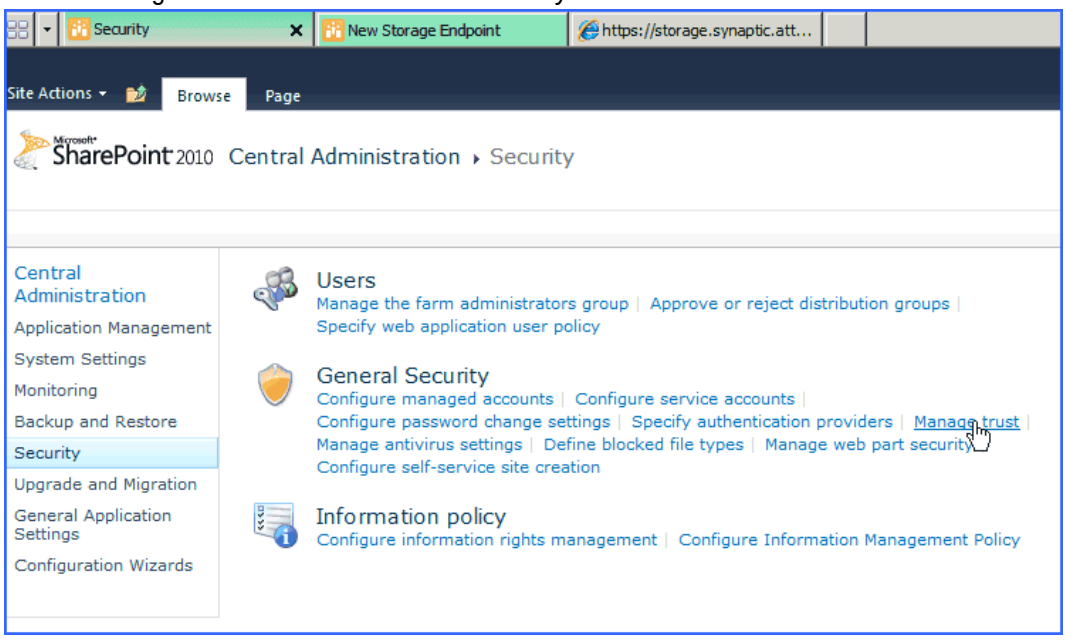
7. Open the certificate. On the Details tab, click Copy To File...



8. The Certificate Export Wizard opens. Click Next. The default "DER" format is fine. Save to the desktop as something like verisign-G5-root.cer. Click Next.

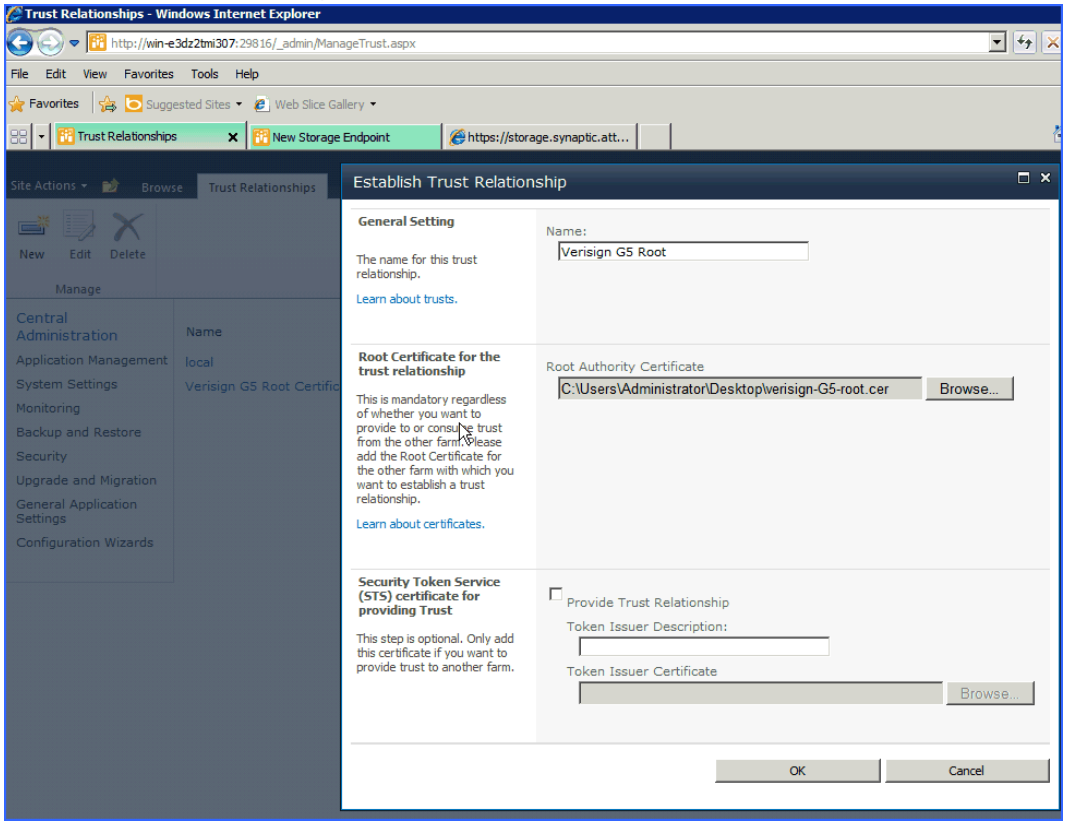
9. Click Finish to complete the export. Click OK on the message. Click OK to close the certificate window.

10. Open the SharePoint Central Administration. Click Security from the navigation on the left. Select Manage Trust from the General Security section.



11. You will probably only see one certificate here, "local". Click "New."

12. Give it a name like Verisign G5 Root. Pick the file you exported to your desktop. Leave "Provide Trust Relationship" blank.



13. Click OK.

The Use SSL option can now be configured and used with the StoragePoint EMC Atmos adapter.

Appendix: Atmos adapter support for TLS 1.1

The following steps need to be performed on all servers that have StoragePoint installed.

1) Install MS fix for TLS for .NET 3.5:

https://support.microsoft.com/en-us/help/3154519/support-for-tls-system-default-versions-included-in-the-net-framework

Support for TLS System Default Versions included in the .NET Framework 3.5 on Windows Server 2012

Applies to: Windows 8, Windows Server 2012 Datacenter, Windows Server 2012 Datacenter, More

The .NET framework version 3.5 and earlier versions did not provide support for applications to use Transport Layer Security (TLS) System Default Versions as a cryptographic protocol. This update enables the use of TLS v1.2 in the .NET Framework 3.5.

Resolution

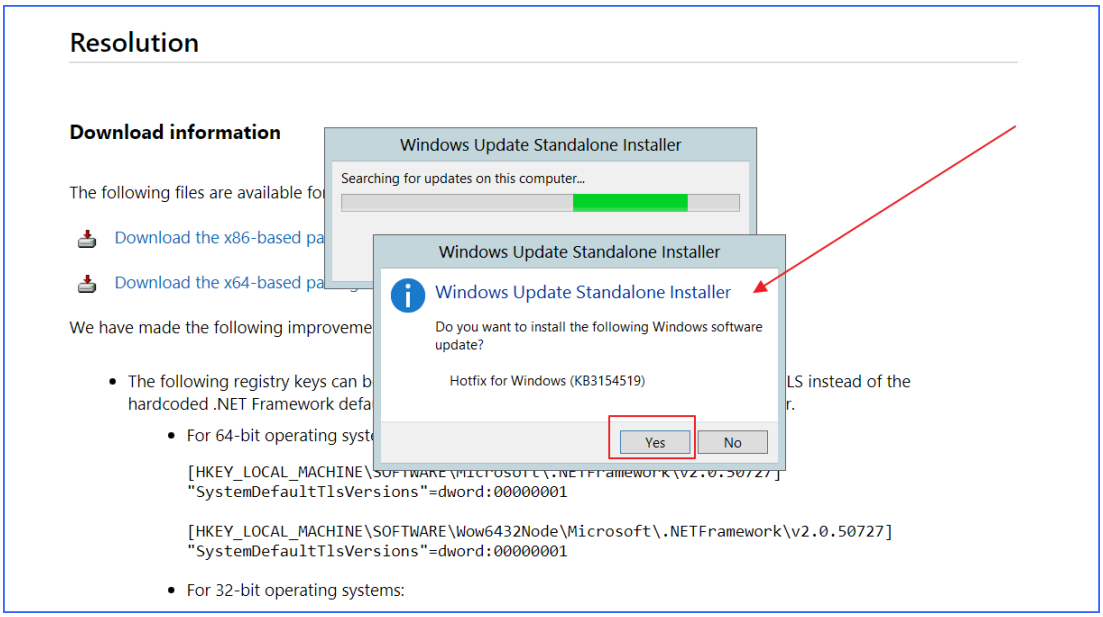
Download information

The following files are available for download from the Microsoft Download Center:

Download the x86-based package now.

Download the x64-based package now.

We have made the following improvements in this area:



Resolution

Download information

The following files are available fo

Download the x86-based pa

Download the x64-based pa

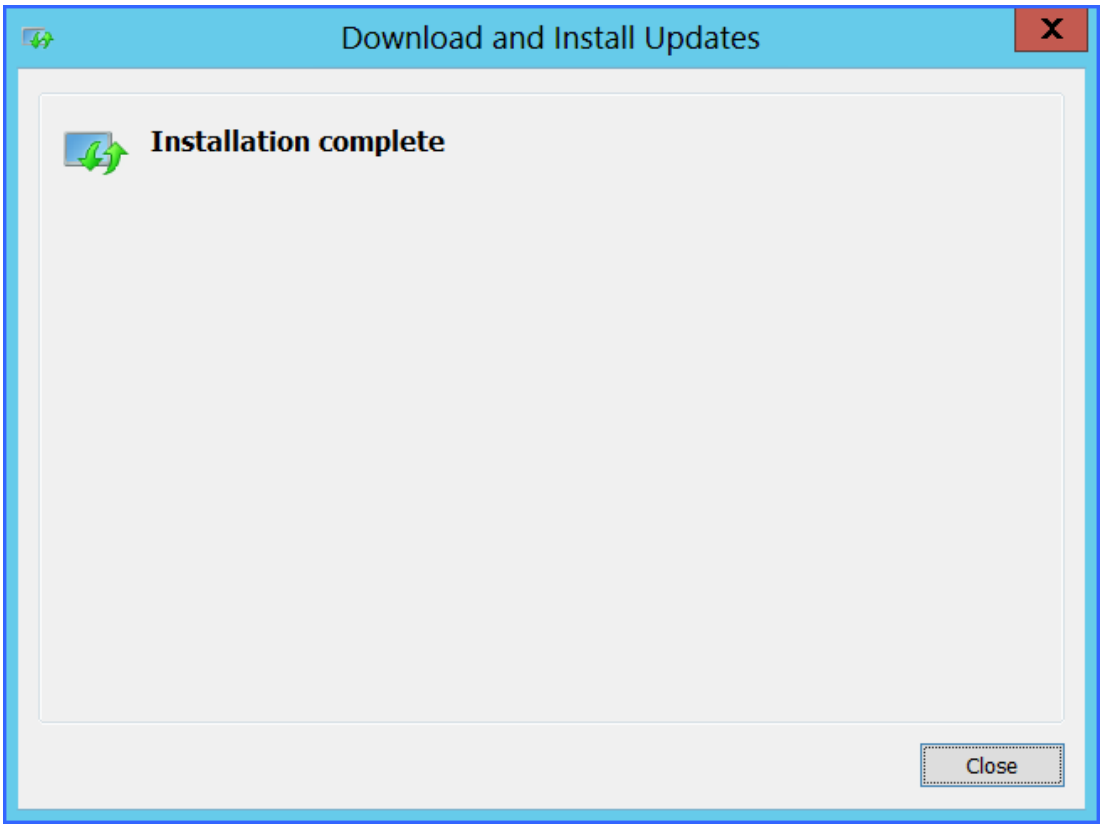
We have made the following improveme

- The following registry keys can b LS instead of the hardcoded .NET Framework defa r.
  - For 64-bit operating syst

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v2.0.50727]
"SystemDefaultTlsVersions"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727]
"SystemDefaultTlsVersions"=dword:00000001
```

  - For 32-bit operating systems:



2) Provide defaults for TLS configuration (in this case TLS 1.1). Add the following registry values (if missing):

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v2.0.50727]
"SystemDefaultTlsVersions"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727]
"SystemDefaultTlsVersions"=dword:00000001
```

3) Verify if TLS 1.1 client is enabled:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client]
"Enabled"=dword:00000001
"DisabledByDefault"=dword:00000000
```

4) Complete an IIS reset and SP Timer Service Reset.

5) Test on Atmos endpoint web page.

6) Run the BLOB Health Analyzer job for requested profile(s).

2

About Us

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece — you — to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

Technical Support Resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles

- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product