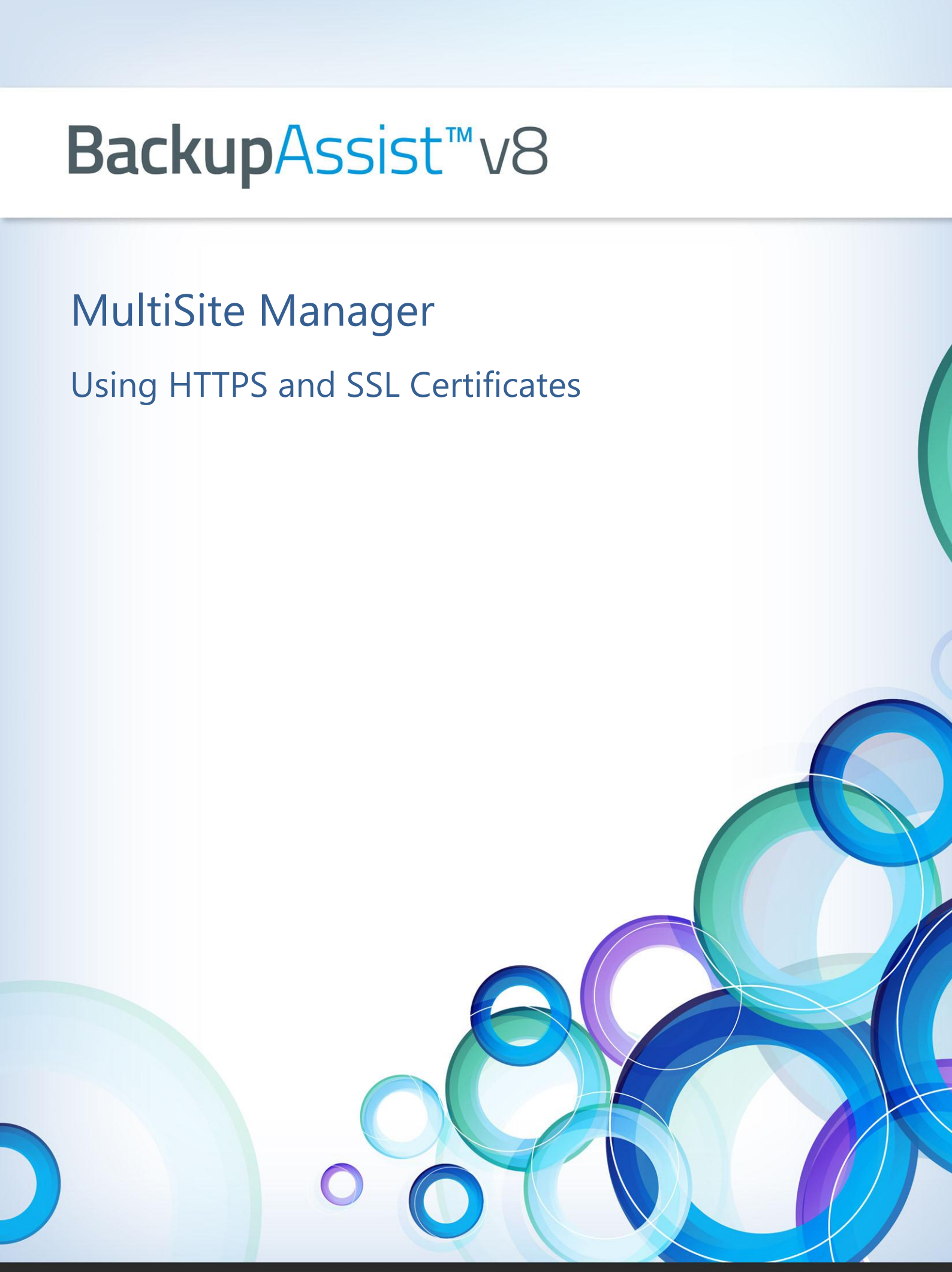
BackupAssist™ v8

MultiSite Manager

Using HTTPS and SSL Certificates



Cortex I.T.

Contents

1. Using HTTPS

BackupAssist MultiSite Manager is used to remotely administer BackupAssist computers. The computers are grouped into sites and one computer in each site is made a Site Controller. The Site Controller connects to the MultiSite Manager and communicates on behalf of its site.

The communication takes place at two levels:

- Within a site (LAN)
- Between a Site Controller and the MultiSite Manager (WAN)

Both or either of these levels of communication can be secured using the HTTPS option.

To go directly to the section that explains How to Create a Self-Signed Certificate, click here.

What is HTTPS

HTTPS is a secure version of the HTTP protocol that uses TSL/ digital certificates to create a secure connection.

A certificate is like an ID card that proves the identity of the host or server. A client that connects to the server (e.g. web server) has a list of the certificates and certificate issuers that it trusts.

When a server sends a client a certificate to initiate a secure connection, the client can verify the certificate by using its trusted list to determine if it trusts the certificate and that the certificate is legitimate.

The advantages of certificates

- The certificate confirms that the server can be trusted and that it is who it says it is.
- A trusted connection uses encryption so that information is not sent as clear text over the internet.

Where to implement HTTPS

The first decision is where to enable HTTPS to secure your MultiSite Manager communications - within a site (LAN), between the Site controller and Multisite Manager (WAN), or at both levels.

- For a LAN - the communication within the site occurs between the BackupAssist computers and the Site Controller. This communication is inside your own network, so you do not have to use HTTPS. If you do, you can create your own digital certificate.
- For a WAN - the communication between sites occurs between a Site Controller and a MultiSite Manager. This communication takes place over the internet, so you SHOULD use HTTPS. You can create your own digital certificate or purchase a globally trusted certificate.

MultiSite Manager HTTPS (TSL/SSL) options

Level	Between	Over	HTTPS
Within a LAN	Computers & Site Controller	Local network	Can be used
Across a WAN	Site Controller & MultiSite Manager	Internet	Should be used

2. How to enable HTTPS in MultiSite Manager

Enabling HTTPS involves two steps. Selecting it for LAN / WAN and then telling the computers at that level to use HTTPS when they communicate.

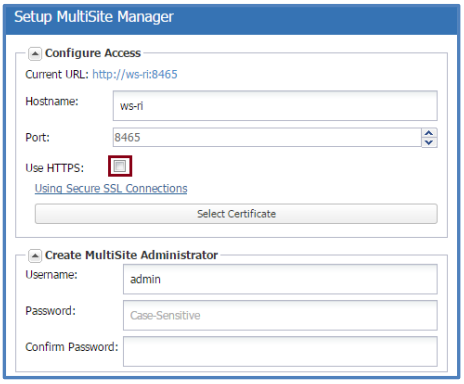
To enable HTTPS across the WAN

1) Enable HTTPS in MultiSite Manager.

When you run Multisite Manager for the first time, you will be presented with a setup window containing the option *Use HTTPS*.

Tick this box and Multisite Manager will only accept HTTPS communication.

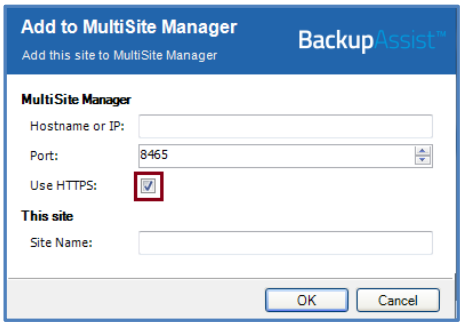
You can also access *Use HTTPS* from the *Welcome* menu by selecting *Edit Setup* > *Use HTTPS*



2) Set each Site Controller to Use HTTPS.

When you register a Site Controller, the final step is the *Add to MultiSite Manager* window, which includes the option *Use HTTPS*.

Select *Use HTTPS* and the Site Controller will only communicate with the MultiSite Manager using HTTPS.



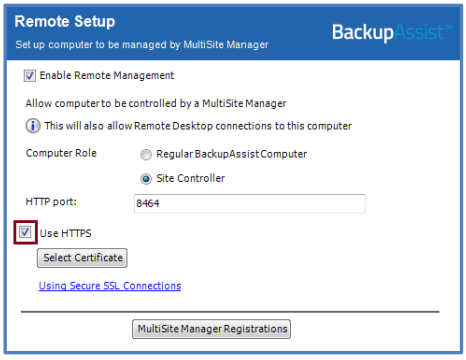
To enable HTTPS within a LAN

1) Enable HTTPS on the Site Controller.

When you assign a BackupAssist computer the Site Controller role using the *Remote Setup* window, a new option will appear called *Use HTTPS*.

Tick this box and the Site Controller will require HTTPS communication within the site.

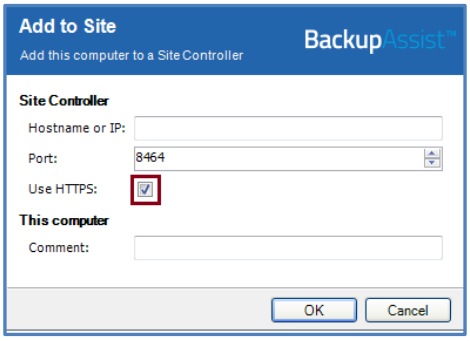
Remote Setup is accessed from the BackupAssist *Remote* tab



2) Set each computer to Use HTTPS.

When you register a computer to a Site Controller, the final step is the *Add to Site* window, which includes the option *Use HTTPS*.

Select *Use HTTPS* and the BackupAssist computer will only communicate with the Site Controller using HTTPS.



3. Selecting a HTTPS SSL certificate

When you enable HTTPS at the MultiSite Manager (WAN) level or the Site Controller (LAN) level, the **Select Certificate** button will become active. This is used to select the digital certificate that SSL/TSL will use to secure your HTTPS communications.

There are two types of certificates:

- A certificate that you purchase from a trusted issue. This will be trusted globally.
- A self-signed certificate that you make yourself. This will be trusted within your organization.

The type you use will depend on your company's security requirements and who will need access.

- WAN enabled HTTPS connections use the MultiSite Manager's certificate. The Site Controller and the client accessing the MultiSite Manager's Web application must both trust the certificate.
- LAN enabled HTTPS connections use the Site Controller's certificate. The BackupAssist computers must trust the certificate.

Trusted issuer certificates

Trusted issuers are companies that sell globally trusted certificates. Annual payments are required for the company's ongoing work to ensure the certificate is secure and that all certificates it issues are trusted. These certificates will come with instructions on their implementation and use.

If you think of a certificate as an ID card, these certificates are like passports issued by governments because they are trusted globally. When anyone in the world sees the passport, they will accept it as evidence that you are who you say you are, because the passport was issued by a trusted entity.

The Windows client maintains a list of certificate issuers that they trust. The client will trust any certificate supplied by a certificate issuer in this list.

Purchasing a certificate from trusted issuer is ideal for a web application that wants to provide secure connections to computers all over the internet. It is recommended that the MultiSite Manager WAN level communications (over the internet) use a certificate issued by a trusted issuer.

Self-signed certificates

These are certificates that you create yourself for free, using the Microsoft Management Console (MMC) or the Microsoft Internet Information Services (IIS). An example of how to create a self-signed certificate using the IIS is provided in the next section.

A new self-signed certificate will not exist in any computer's trusted certificates list. This means that once the self-signed certificate has been created, you will need to tell each computer that they can trust the certificate when they make their first connection. Web browsers will also need to trust and install a certificate when they make a connection.

Self-signed certificates are ideal for a company that wants to create a secure connection within its own organization because it knows it can trust its own self-signed certificate, and it can configure its company computers to trust the certificate.

If you want to have secure connections with in a site's LAN (between the Site Controller and BackupAssist computers), self-signed certificates would be an appropriate cost free solution.

4. How to create a self-signed certificate

This section explains how to create your own self-signed digital certificate.

- To secure communication between MultiSite Manager and each Site Controller (WAN level), the certificate must be created on (or imported to) the computer that MultiSite Manager is installed on.
- To secure communication between a Site Controller and each computer in the site (LAN level), the certificate must be created on (or imported to) the computer that the Site Controller is installed on.

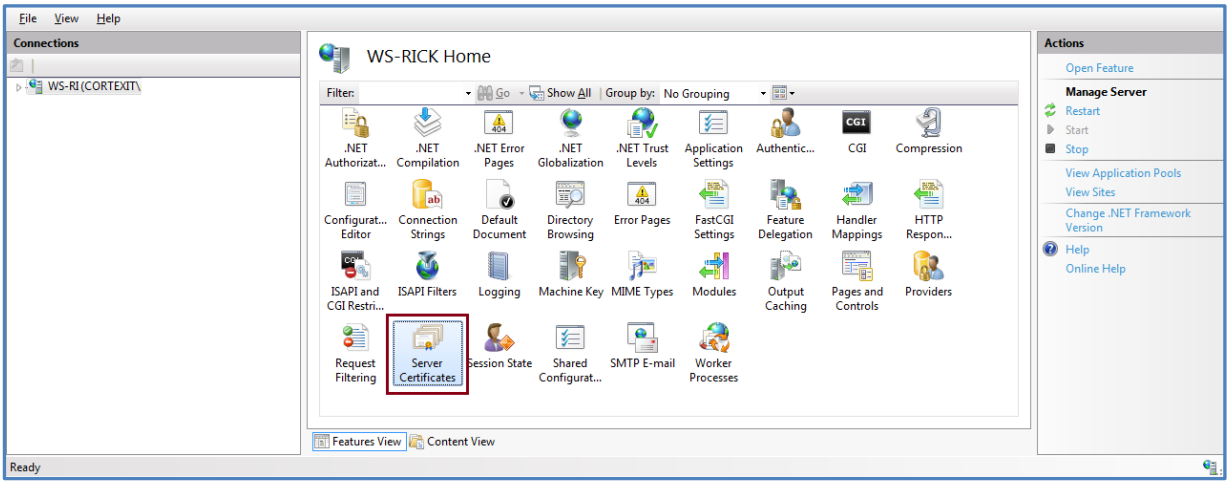
The self-signed certificate creation process shown below uses IIS (Microsoft Information Services).

- To install IIS on a Windows workstation, select the *Control Panel*, *Programs and Features* and under *Turn on Windows Features*, select *Internet Information Service*.
- To install IIS on a Windows Server, go to *Server Manager*, select *Manage*, select *Add Roles and Features*. Follow the steps and select *Web Server (IIS)* from the *Server Roles* list.

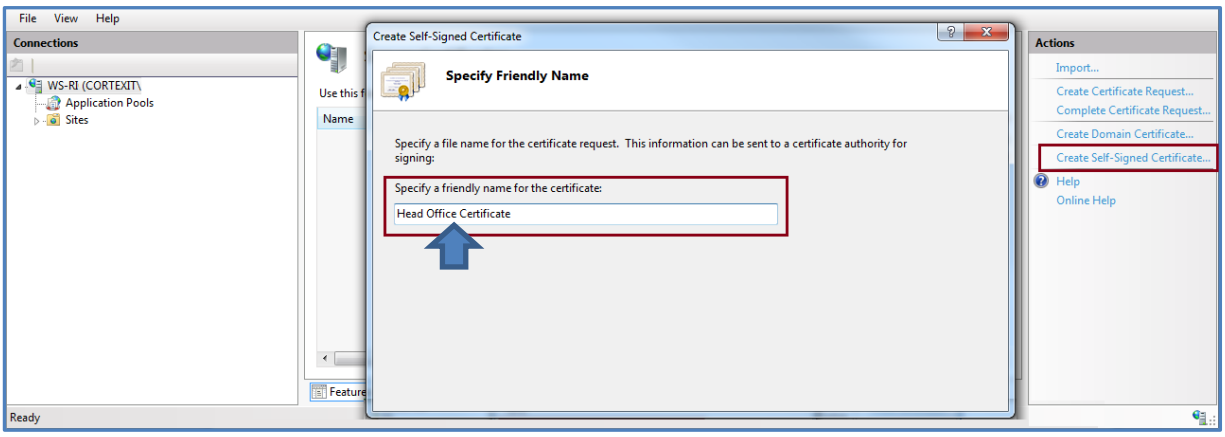
Creating a self-signed certificate

1. Select **Start** and run **inetmgr**.

   This will open the **Internet Information Services Manager** and display the options available.



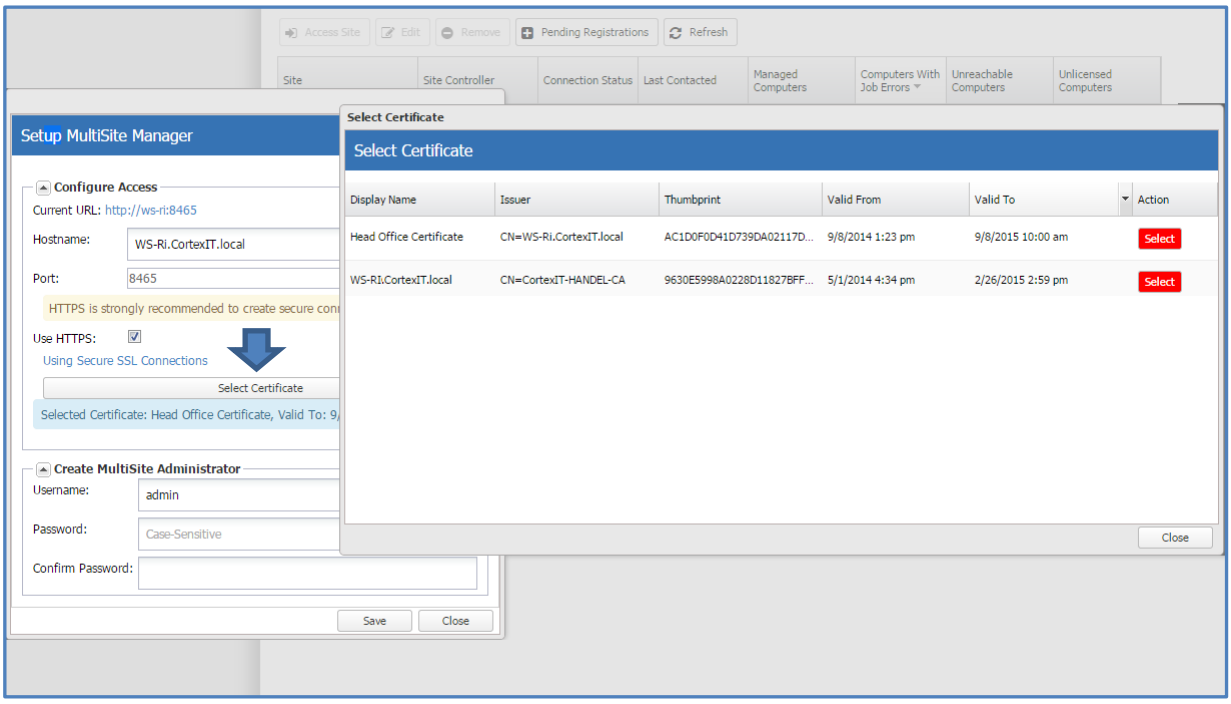
2. Double-click **Server Certificates**.
3. From the right panel select **Create Self-Signed Certificate**.



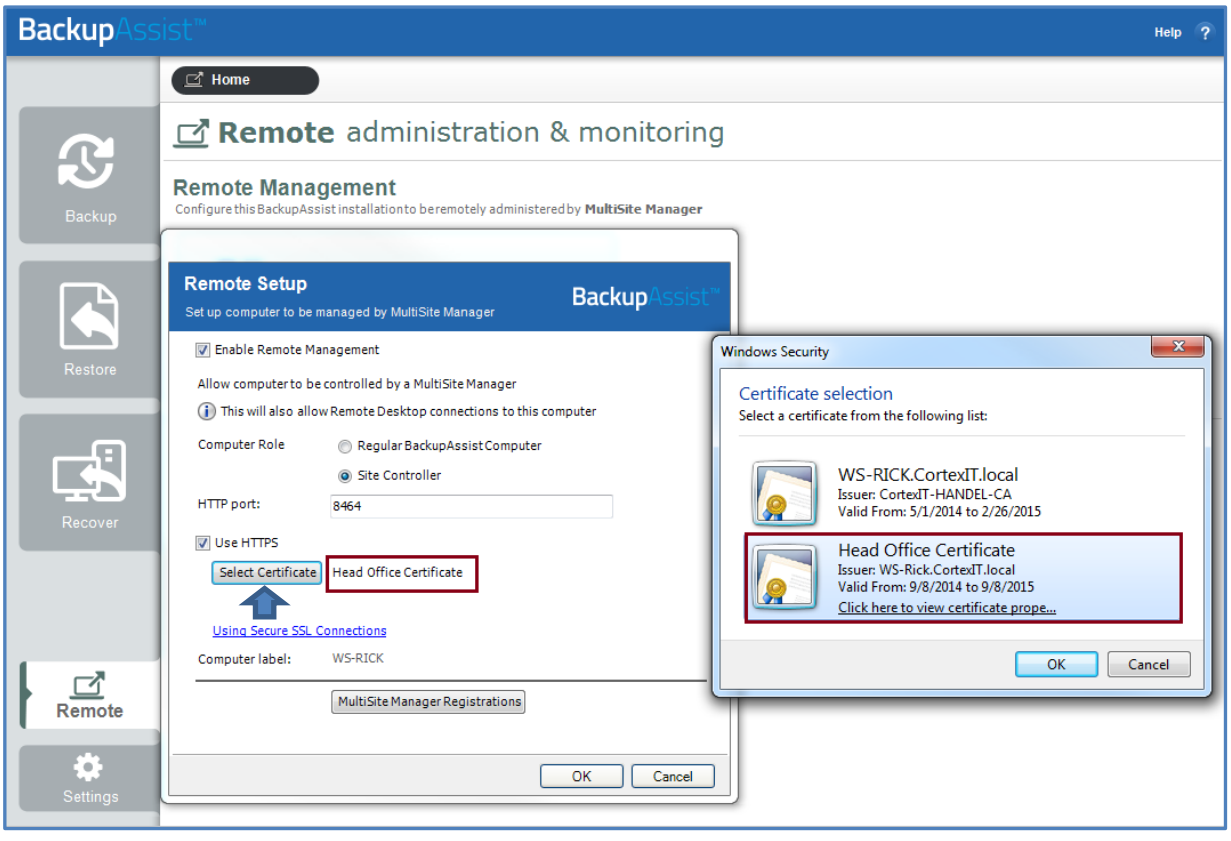
4. Enter a name for the certificate and select OK
5. If you are using a server operating system, select **Personal** for the certificate store.

Selecting the certificate

On the **MultiSite Manager**, after enabling Use HTTPS, you will be able to select your self-signed certificate through the **Select Certificate** button.



On the **Site Controller**, after enabling Use HTTPS, you will be able to select your self-signed certificate through the **Select Certificate** button.



5. How to trust a certificate

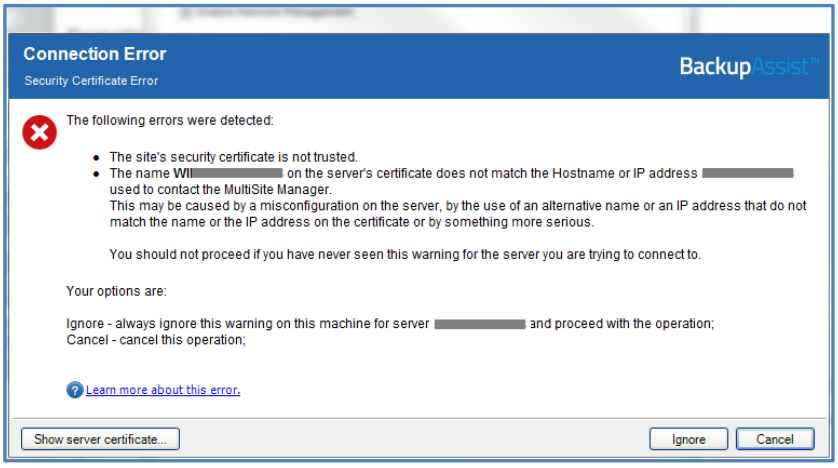
Once a digital certificate has been created (and HTTPS enabled) on the MultiSite Manager, the certificate must be trusted by each Site Controller that connects and communicates with it. Any computer opening the MultiSite Manager web application in a browser must also trust the certificate. And if the Site Controller has created a certificate (and enabled HTTPS) each computer in that site must trust that certificate.

- Each Site Controller must trust the MultiSite Manager's certificate.
- Each BackupAssist computer must trust the Site Controller's certificate.
- The computer opening MultiSite Manager using a browser must also trust the certificate.

Trusting a Site Controller certificate (LAN)

When you use BackupAssist to add a Regular BackupAssist Computer, to a Site Controller, and select *Use HTTPS* in the *Add to Site* window, a warning will appear when you select OK. The warning explains that you have selected *Use HTTPs*, but your computer does not yet trust the Site Controller's certificate.

1. Select **Show server certificate**, to check it is the correct certificate.
2. Select **Ignore** and the BackupAssist computer will trust the Site Controller's certificate.



Trusting a MultiSite Manager certificate (WAN)

When you use BackupAssist to register a Site Controller to a MultiSite Manager, and select *Use HTTPS* in the *Add to MultiSite Manager* window, a warning will appear when you select OK. The warning explains that you have selected *Use HTTPs*, but the Site Controller does not trust the MultiSite Manager's certificate.

3. Select **Show server certificate**, to check it is the correct certificate.
4. Select **Ignore** and the Site Controller will trust the MultiSite Manager's certificate.

Web browsers trusting a certificate

If you attempt to open MultiSite Manager using a web browser that does not trust the MultiSite Manager's certificate, then the connection will fail and the browser will display a warning / error message. After ensuring that the details of the certificate is correct, you can accept the warning and

allow the browser continue and add the certificate to clients/browser's trusted list. The process will vary from web browser to web browser. Where the certificates are stored depends on the browser.

Hostname compatibility

The hostname in the URL used to open MultiSite Manager must match the hostname in the certificate's FQDN. If they do not match, you will get a security warning that the connection is not trusted

The MultiSite Manager setup dialog can be used to update the hostname used to access the MultiSite Manager, to ensure that it matches the hostname in the certificate's FQDN.

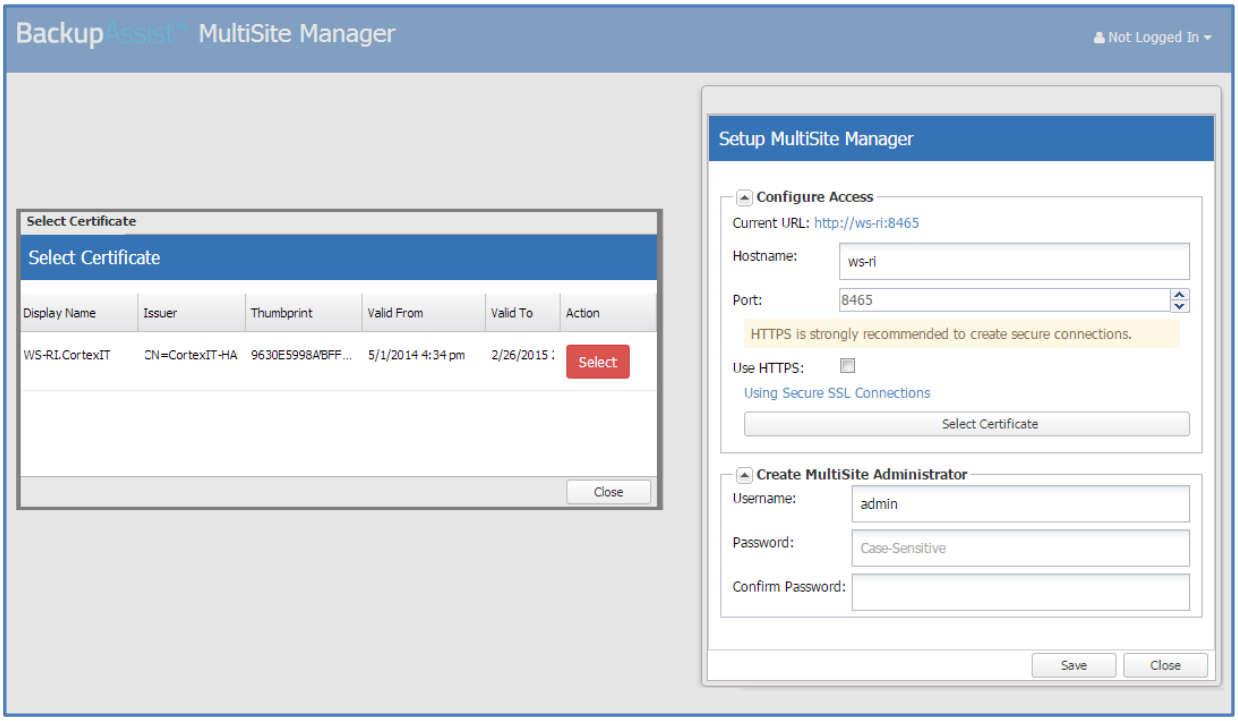


Figure 1MultiSite Manager setup and SSL certificate selection

NOTE: If you enter an invalid hostname, MultiSite Manager will not open. If this happens, you can manually modify the path in the browser's address bar and log in to MultiSite Manager again. Then change the hostname in the Edit setup screen. .