October 13th, 2021

Contents

1 Introduction

The **Impero WebConnect** service is a secure web-based solution consisting of a **Connection Manager** that serves as a meeting hub for the **Impero Guests** and **Hosts**, and at least one **Connection Server** that routes the traffic between the **Guests** and the **Hosts**. Using the **Impero WebConnect** service, users can remote control computers without having to configure any firewall(s), proxy(s) or router(s).

Impero WebConnect communication is normally used to connect a **Guest** to a **Host** across the internet where they are typically separated by firewalls and the IP address of the **Host** may be unknown. When using the **Impero WebConnect** service users can remote control computers typically without having to configure any firewall, proxy or router. This is because **Impero WebConnect** can rely on outbound HTTP traffic on port 80 from the **Guest** and **Host** (including **Impero OnDemand Hosts** and **Impero Mobile Hosts**).

In addition to using HTTP on port 80, **WebConnect** can be configured to use a pure TCP protocol on port 6502 (or on the port you choose). By using the TCP protocol you get a significant performance boost, however it can require you to make some allowances on your firewall. When you have both TCP and HTTP protocols enabled for your **WebConnect** environment, it first tries the faster TCP protocol and if that does not succeed it falls back to HTTP.

To use **WebConnect** on the internet, both the **Connection Manager** and **Connection Server** must have a public IP address where routing or port forwarding is used to reach the service. It is recommended that you use a separate computer for the **Connection Manager** and each **Connection Server**. Although it is not required, many customers choose to install the **WebConnect** modules on servers placed in their **DMZ**.

The **Connection Manager** uses *Microsoft Internet Information Service* and relies on the connectivity to a *Microsoft SQL* database for data management. The **Connection Manager** facilitates connection information and parameters to **Impero Guests** and **Hosts** when they meet and it assigns them a **Connection Server** to use as a communication relay. For best performance, it is recommended that the **Connection Manager's** ODBC connection is to a Microsoft SQL database running on a separate, more powerful server. If **WebConnect** is intended for use in a high load, enterprise environment, then the database connection should be to an SQL environment that uses load balancing (SQL Server 2008 R2 Parallel Data Warehouse Edition) or an SQL clustered environment.

NOTE: If the **Connection Manager's** IIS is configured with a certificate from a certificate authority to support SSL then the **Guest** and **Host** can communicate with the **Connection Manager** using HTTPS:443 in addition to HTTP:80.
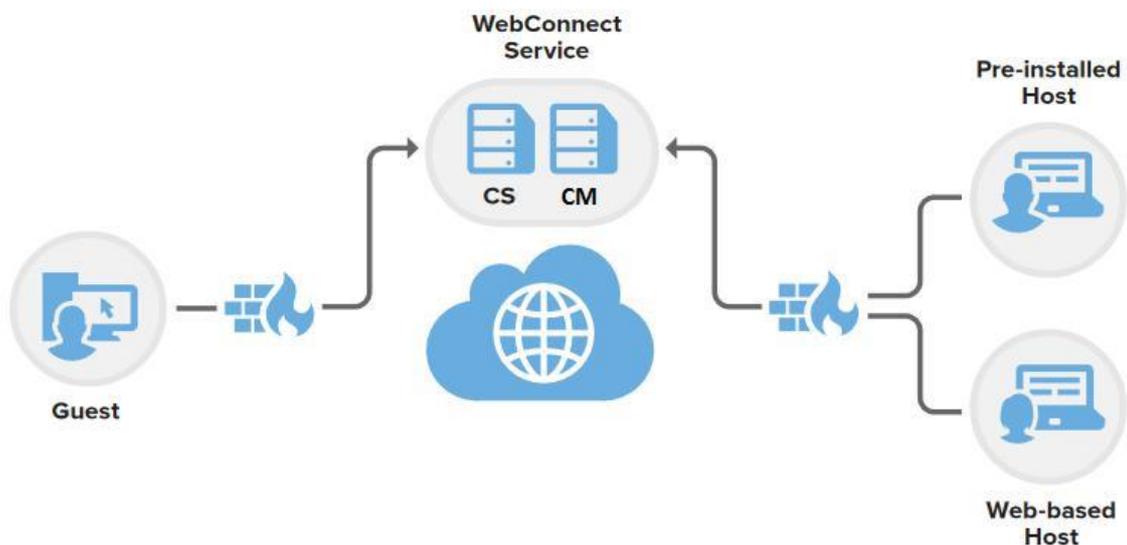
Scope of Document

This document is intended to guide the user through the installation steps of the **WebConnect** service.

Prerequisites

This section provides the basic prerequisites. For the detailed **WebConnect** prerequisites, technical specifications and recommendations, refer to the Impero Knowledge-base.

Connection Manager

Platforms (32-bit and 64-bit):

- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2008
- Windows Server 2008 R2 (all editions)

Microsoft Internet Information Services 6.0 or higher- default installation with the following extra items:
  - o IIS service roles required to be enabled:
    - *IIS 6 Metabase Compatibility*
    - *ISAPI Extensions*
- ODBC connection to Microsoft SQL Server 2005 or higher

Hardware specifications

- Windows 64-bit OS
- Intel Quad-Core processor (or better)
- A minimum of 8 GB RAM
- Gigabit Ethernet connectivity to the SQL Server and the Connection Servers
- 7,200 RPM (or faster) hard drive

Connection Server

Platforms (32-bit and 64-bit):
- Windows Server 2016,
- Windows Server 2012,
- Windows Server 2012 R2,
- Windows Server 2008
- Windows Server 2008 R2 (all editions)

Hardware specifications

- Intel Quad-Core processor (or better)
- A minimum of 8 GB RAM
- Gigabit Ethernet connectivity to the Connection Manager
- 7,200 RPM (or faster) hard drive

SQL Server: Microsoft SQL Server 2005 or higher

Hardware specifications

- Intel Quad-Core processor (or better)
- A minimum of 16 GB RAM
- Gigabit Ethernet connectivity to the Connection Manager
- 2 x 7,200 RPM (or faster) hard drive in RAID0 or similar, 2 x 10.000 RPM HDD in RAID 0 or similar, or 1 SSD hard drive

Recommendations

At a minimum, two computers are necessary. One computer for the Connection Manager and another computer for the **Connection Server**. **The Connection Manager and each Connection Server must have their own unique public IP address.** In low volume environments, the SQL database can reside on the same computer as the **Connection Manager**.

For high volume environments of greater than 1,000 **Hosts**, it is required that the database resides on a separate SQL server. For even better performance the SQL database should be in an SQL server load-balanced environment. As the number of **Hosts** grows, it also may also be necessary to consider additional **Connection Managers** running in a web server load-balanced environment.

Additional **Connection Servers** can be added depending on the number of required concurrent connections between the **Guest** and **Host** through the **WebConnect** service. It is recommended that you have at least one **Connection Server** for every twenty concurrent connections. If the

requirement is to support one hundred concurrent connections, at least five **Connection Servers** are necessary.

2 Impero WebConnect Connection Manager setup

The **Connection Manager** facilitates connection information and parameters to the **Impero Guests** and **Hosts** that have a need to meet in relation to remote control sessions. It enables ad-hoc secure connections between the **Impero Guests** and **Hosts**.

The **Connection Manager** directs the clients to a **Connection Server** that handles the actual routing.

The **Connection Manager** uses Microsoft Internet Information Server (IIS) and Microsoft SQL Server for data management.

The following illustration displays the security architecture of the **WebConnect** system:
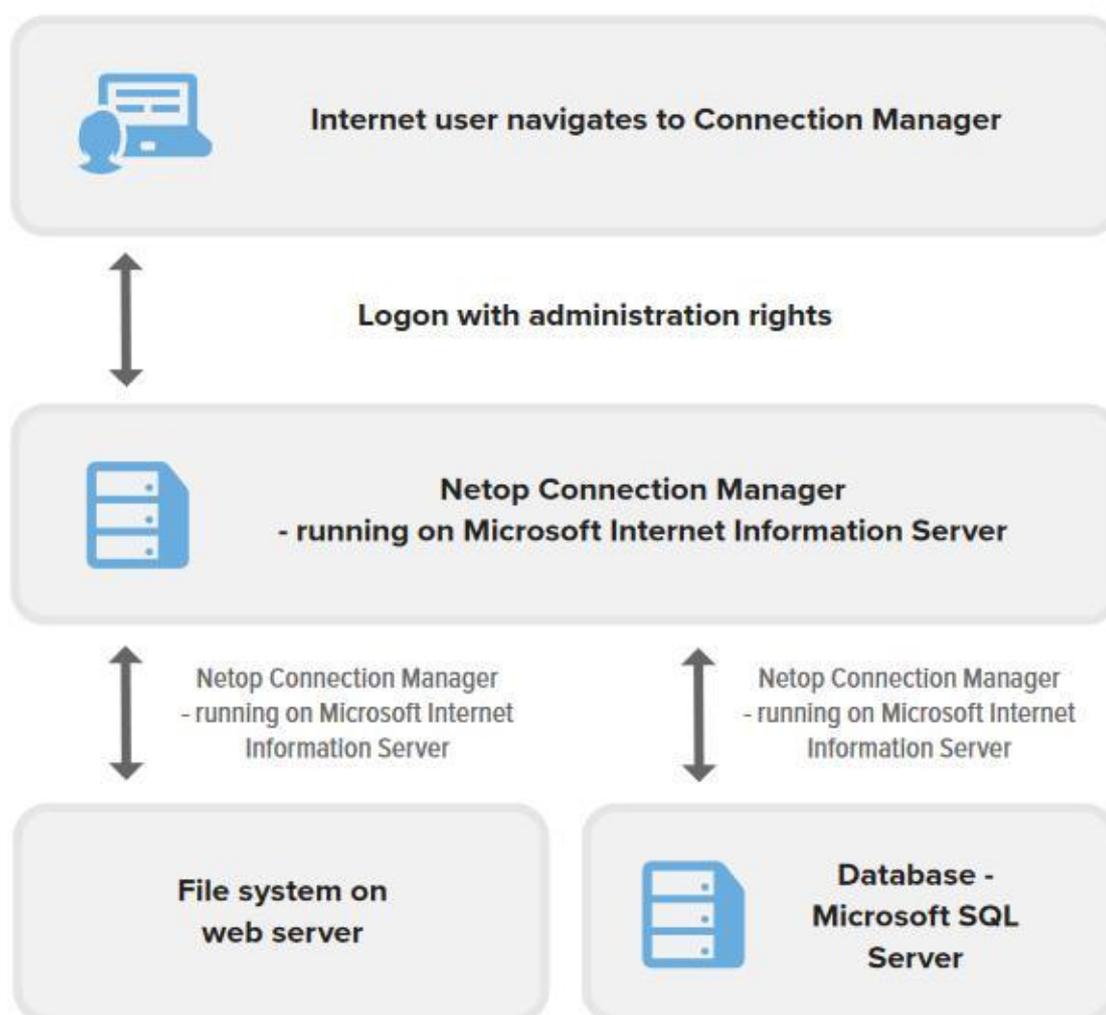
The **Impero WebConnect Database Wizard**, which is displayed during installation, handles the setup illustrated above, including the setup of the IIS. If you want to use a domain user instead of the local IUSR specified above, you need to set up the rights for the user.

Refer to the Microsoft Internet Information Server (**IIS**) documentation for more information on how to configure the **IIS**.

If the database engine (SQL Server) is executed on the same machine as the IIS/ISAPI application, verify that the database connection is set up correctly to use the local database.

The following sections describe:

- How to install the **Connection Manager** and configure the database
- How to configure the **Connection Manager**
- The activity log that records all the activity and logon attempts
- Some useful optional tools to optimize your system

2.1 Install the Connection Manager and configure the database

The installation and configuration process varies depending on whether you want to install the **Connection Manager** and SQL database on the same machine or on two different machines.

If the **Connection Manager** and the SQL database are installed on the same machine, proceed as follows:

1. Copy the installation files (vcredist_x86 folder including the **.exe** file, Connection Manager.msi, setup.exe) to the machine on which you want to install the **Connection Manager**.
2. Run the **setup.exe** file.

3.   Follow the on-screen instructions to complete the installation. During the installation, you are prompted to configure the database in the **Database Wizard.**
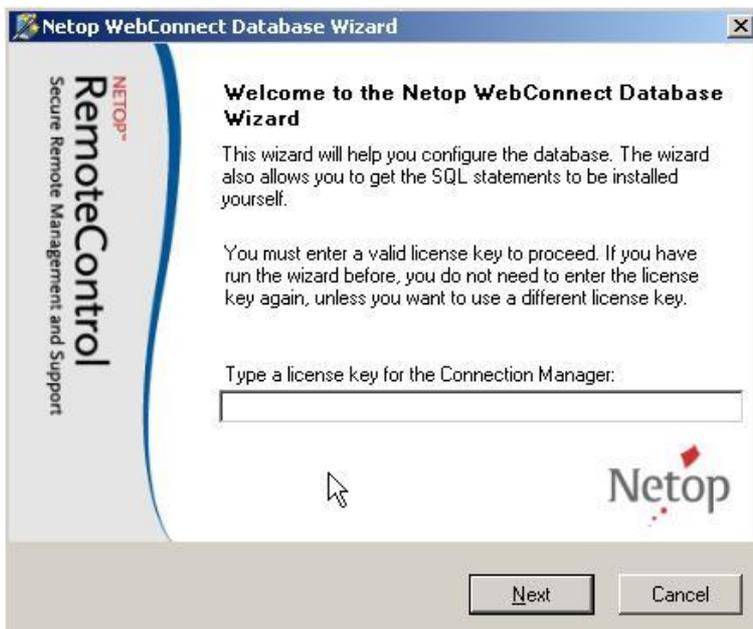
4.Specify a valid license key for the **Connection Manager**.

5.Click on **Next**.

NOTE: If you decide to run the **Database Wizard** again from the **Start** menu, it is not necessary for you to specify the license key for the **Connection Manager** again.

6.From the **Select database server** page, you can download a test database (SQL Server 2005/2008 Express) from Microsoft if you select the **Download database for test** checkbox, click on **Next** and click on the first link to download SQL Server 2005/2008 Express. If SQL Server is installed, do not select the **Download database for test** checkbox.

7.Click on **Next**.

In the **Database configuration** page you can either use the easy setup or the advanced configuration:

- If you select the **Use default setting**, you are taken to the final page of the **Database Wizard.** Click on **OK** to finish the setup.

- If you select to use a more advanced configuration (**Use default setting** is unselected) when you close the **Data Link Properties** dialog box the **Edit values for connecting to SQL** page is displayed.

  - Based on your SQL database setup, select **Use a Windows NT user** or **Use an SQL account**.

  - Optionally, to see and/or copy the SQL statements to your preferred SQL editor and then edit and execute them, select the **View and edit SQL statements** checkbox.

8. Click on **Next**.

9. Click on **OK** to complete the wizard.

NOTE: For security reasons, passwords in the database are scrambled to prevent intruders from being able to read them.

If the **Connection Manager** and SQL database are installed on two different machines, proceed as follows:

1. Before you install **WebConnect** on the SQL server, select **Security** > **Logins** > **sa**.

2. Right-click on **sa**.

3. Select **Properties** > **Status.**

4. Enable the user.

5. Click on **OK**.

NOTE: If you have a firewall on the target SQL Server, open port **1433** (default).

6. Copy the installation files (vcredist_x86 folder including .exe file, Connection Manager.msi, setup.exe) to the machine on which you want to install the **Connection Manager.**

7. Run the **setup.exe** file.

8. Follow the on-screen instructions to complete the installation.

9. Specify a valid license key for the **Connection Manager** and click on **Next**.

10. Click on **Next**.

11. Make sure that the Use default setting is not selected.

12. Click on Next.

13. Set the **Data Link Properties**:

13.1.	Specify the IP address of the SQL Server. If you are connecting to an SQL instance, also specify the instance name, for example, 192.168.1.1\instancename.

13.2.	Select **Use a specific user name and password.**

13.3.	Enter the **sa** account details from the SQL Server.

13.4.	Select to **Allow saving password**.

13.5.	Leave empty the **Select the database on the server** field.

13.6.	To verify your settings, click on the **Test Connection** button.

13.7.	Click on **OK** to continue.

14. Select **Use an SQL account**.

15. Specify the credentials of a new user that the IIS uses on the SQL database for **WebConnect**.

NOTE: Optionally, to see and/or copy the SQL statements to your preferred SQL editor and then edit and execute them, select the **View and edit SQL statements** checkbox.

16. Click on **Next**.

17. Click on **OK** to complete the wizard.

Activate the script to tidy up the log

To clean up the log, activate the installed script manually.

To manually activate the script, proceed as follows:

1. In Windows Server, go to **Start** > **Administrative Tools** > **Services**.

2.	In the right pane of the **Services** window, right-click on **SQL Server Agent.** The **SQL Server Agent Properties** window is displayed.

3. In the **General** tab, from the **Startup type** drop-down, select **Automatic**.

3. Below the **Service status** section, click on the **Start** button.

4.Click on **OK**.

NOTE: This applies to SQL Server only. If you are running SQL Server Express, the **SQL Server Agent** is not available.

Set up monitoring of Connection Servers

A **Connection Server** can stop responding for various reasons. To receive notifications by email about non-responsive **Connection Servers**, set up the monitoring of **Connection Servers** in SQL Server Management Studio.
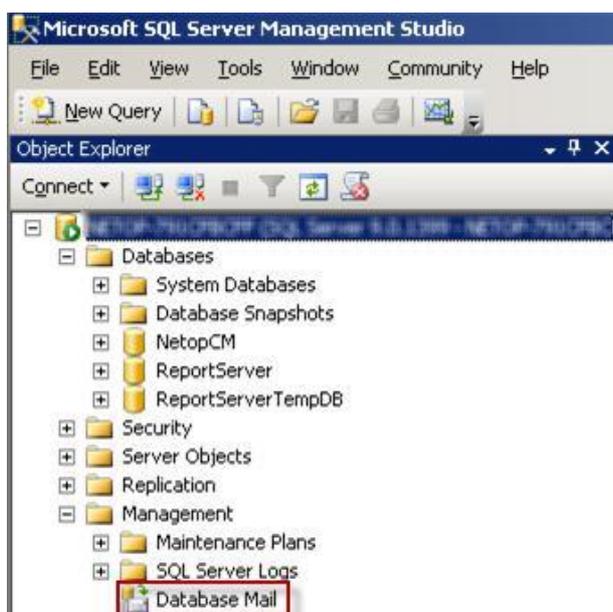
To set up the **Database Mail**, proceed as follows:

1.In the left pane of SQL Server Management Studio, go to **Management.**

2. Right-click on **Database Mail.**

3. Double-click on **Configure Database Mail**. The **Database Mail Configuration Wizard** is displayed.

4.Click on **Next**.

5.Select **Set up Database Mail by performing the following tasks.**

6.Click on **Next**.

7. In the **Profile Name** field, specify a profile name.

8. In the **Description** field, specify a mail profile description for monitoring the **Connection Server**.

9. Click on the **Add** button, to add an SMTP account.

10. Click on the **New Account** button.

11. In the **New Database Mail Account** dialog box, make the following settings:

    11.1. In the **Account name** field enter an account name.

    11.2. Specify an **Outgoing Mail Server (SMTP)** by entering the email address, a display name, and a server name in the corresponding fields below.

    Tip: We recommend you enter the IP address of the Outgoing Mail Server in the **Server name** field.

    11.3. Select the authentication relevant for your SMTP server.

    11.4. Click on **OK**. The account is listed in the **SMTP accounts** list, in the **New Profile** page.

    11.5. Click on **Next**.

12. Select the **Public** checkbox for the profile you created.

13. Click on **Next**.

14. In the following wizard pages, click on **Next** to finish the mail setup.

15. Click on **Close**.

Edit the SQL Server Agent

1. In the left pane of SQL Server Management Studio, go to **SQL Server Agent** > **Jobs**.

2. Right-click on **CheckCSs.**

3. Select **Properties**. The **Job Properties** dialog box is displayed.

4. In the left pane, click on **Steps**.

5. In the **Job step** list in the right pane select the relevant step.

6. Click on **Edit**.

7. In the lower right pane, edit the following information:

- Set `@parm_profile_name` = [The profile name you chose during the Database Mail setup].

- Set `@parm_recipients` = [The email address you specified for Outgoing Mail Server during Database Mail setup].

8. Click on **OK.**

9. Close the SQL Server Management Studio application.

NOTE: This applies to SQL Server only. If you are running SQL Server Express, the Database Mail and the SQL Server Agent are not available.

2.2 Configure Connection Manager

The Impero **WebConnect Connection Manager** (http://localhost/ImperoCM) opens in your web browser (for example Internet Explorer) after you complete the **Impero WebConnect Database Wizard**.

Impero **WebConnect** has two administrator accounts, a site administrator account, and a domain administrator account. Logging on as a site administrator allows you to carry out top-level administration such as adding **Connection Servers** and creating sub-domain accounts while logging on as domain administrator allows you to administrate a particular domain and create accounts for the domain. Each domain has its own administrator.

Site administrator

1. Log on to the Connection Manager as admin.

(**Account**: admin, **Password**: admin. **Domain**: admin).

When you log in on the **Connection Manager** as (site) admin, the following screen is displayed:
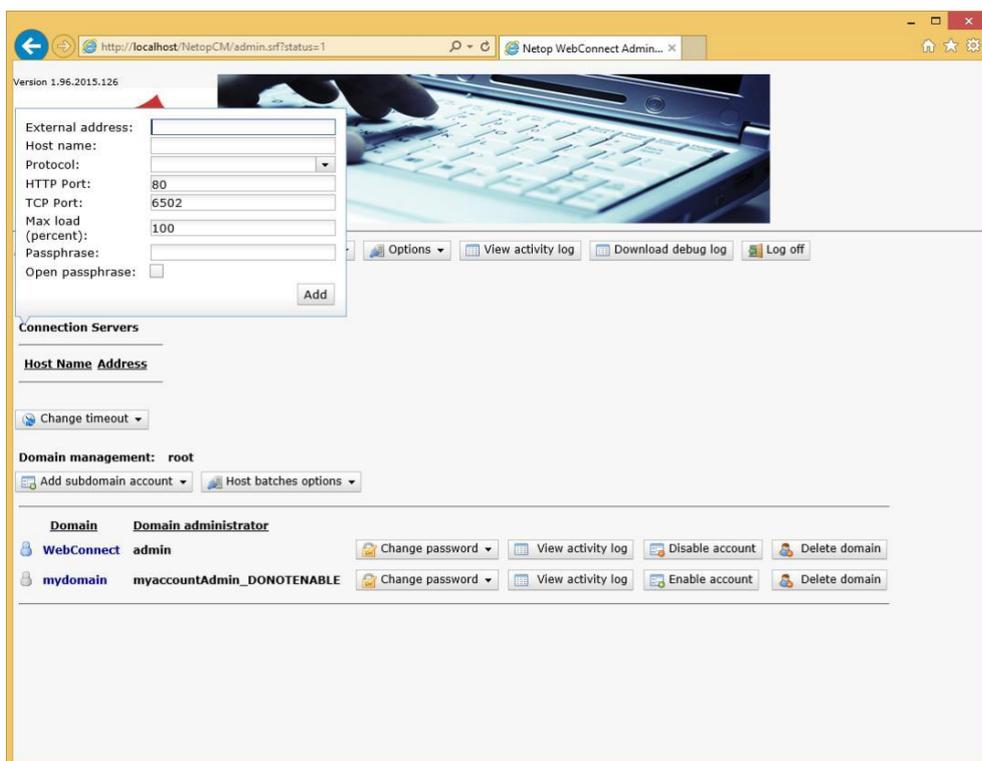
2. To add a **Connection Server**, complete the following fields:

Field	Description
External address	The public-facing IP address for your **Connection Server**.
Host name	Computer name for your **Connection Server**. The name is required in order for the **Connection Manager** to recognize the correct **Connection Server** as the IP address received is not always the same.
Protocol	Select the TCP or HTTP protocol.
HTTP port	If you use the HTTP protocol, define which port to use. The default port is set to **80**.
TCP port	If you use the TCP protocol, define which port to use. The default port is set to **6502**.
Max load (percent)	Specify the maximum connection load in percent that the **Connection Server** handles.
Passphrase	The passphrase is used by the **Connection Manager** to accept communication with the **Connection Server**. If you select the **Open passphrase** checkbox, the **Connection Server** can reset the passphrase.

NOTE: When you change port settings, make sure that your **Connections Servers** are configured to use the same protocols and the appropriate port numbers.
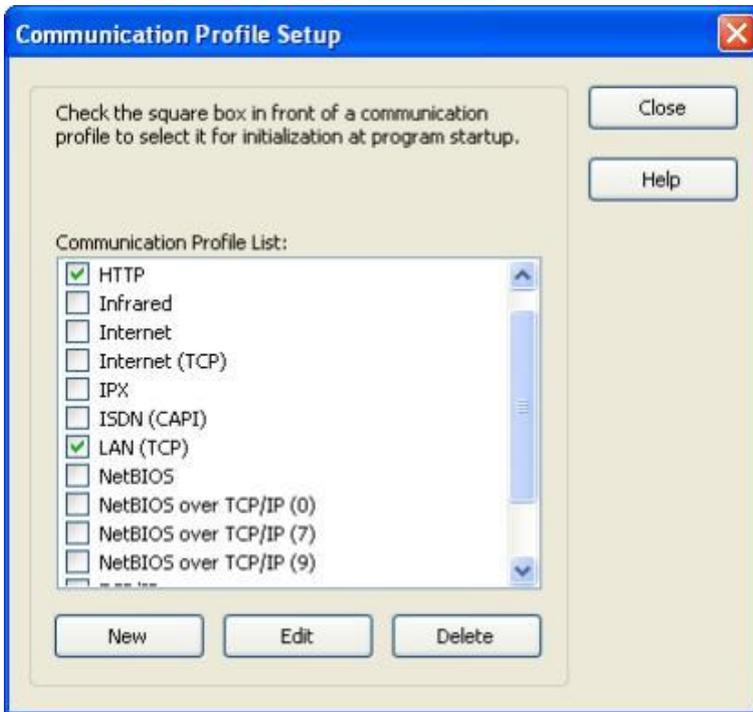
3. Click on **Add** for the changes to take effect.

You can add multiple **Connection Servers**, which are displayed with their IP address in the **Connection Servers** list below.

To edit the **Connection Server** information, click on the **Edit Connection Server** button for the individual servers in the list.

If you no longer want a server to be used, to remove it, click on the **Remove Connection Server** button for the server in the list.

4. Click on the **Change password** tab. Specify a new password and confirm it.
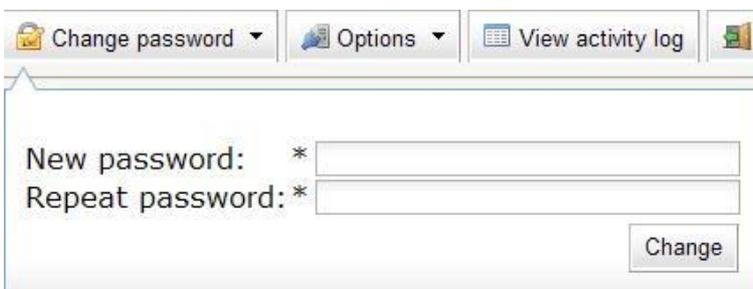
5. Click on the **Change** button for the change to take effect.

6. Click on the **Options** tab to configure the use of secure connections:

6.1. Select the **Require HTTPS** checkbox to use HTTPS for connections. This requires that **SSL** (Secure Socket Layer) be installed.

6.2. Select the Warning when not using **HTTPS** checkbox to have a warning displayed if not using **HTTPS**. This is important because if you select the **Require HTTPS** checkbox and **SSL** is not installed, you cannot return to **HTTPS** and the **Connection Manager** web interface. Therefore, you cannot clear the **Require HTTPS** checkbox again.

NOTE: If you select the **Require HTTPS** checkbox and **SSL** is not installed, you have to change it directly in the database. In the **Global_Config** table, set the value of **NumValue=0** (null) where Name=Require HTTPS. Refer to the Microsoft SQL documentation for further information.

6.3. Click on the **Change** button for the changes to take effect.

7. When you first install the **Connection Manager**, the site contains one default subdomain (**WebConnect**) and the domain admin account (**admin**). This default subdomain and associated accounts can be removed if they are unnecessary.

To create a new domain and domain admin account, proceed as follows:

1. Click on the **Add subdomain account** button and make the following settings:

2. In the **Account** field, enter a domain admin account name.

3. In the **Password** field, enter a password for the domain admin account, and repeat it. You can change the password for the account later by clicking on the **Change password** button for the domain admin account in the **Domain Management** list. You can disable an account by clicking on the **Disable account** button for the account in the **Domain Management** list.

4. In the **Domain** field, enter the name of the new domain.
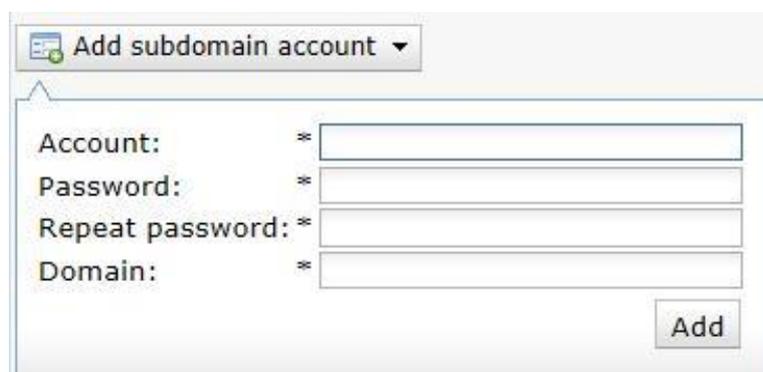
NOTE: Settings marked with * are mandatory.

5. Click on the **Add** button to add the domain account to the **Domain Management** list. It is listed as a domain name - domain administrator.

If your organizational structure consists of a headquarter with subsidiary companies in one or more levels, you can create a structure in the **Connection Manager** which mirrors it by creating subdomains. This allows the **Guests** from a parent domain to inherit the **Hosts** from a child subdomain.

6. To create a new subdomain and domain admin account, click on the **Add subdomain account** button and make similar settings to creating a domain.

About subdomains

To use **Impero WebConnect**, applications require to be configured with account details (username, password, and domain) which are supplied by the **WebConnect** administrators. These accounts are defined in the **WebConnect** subdomains so that each customer (or site) can be completely separate from each other.

For example, if a **Guest** is required to connect to a **Host** using **WebConnect**, both the **Guest** and **Host** have to use the same account from the same domain.

Using subdomains **Guests** from a parent domain inherits the **Hosts** from a child sub-domain. This is particularly applicable for support organizations that are hosting their own in-house **WebConnect** service and require a simple method of managing **Impero** connectivity across multiple sites.
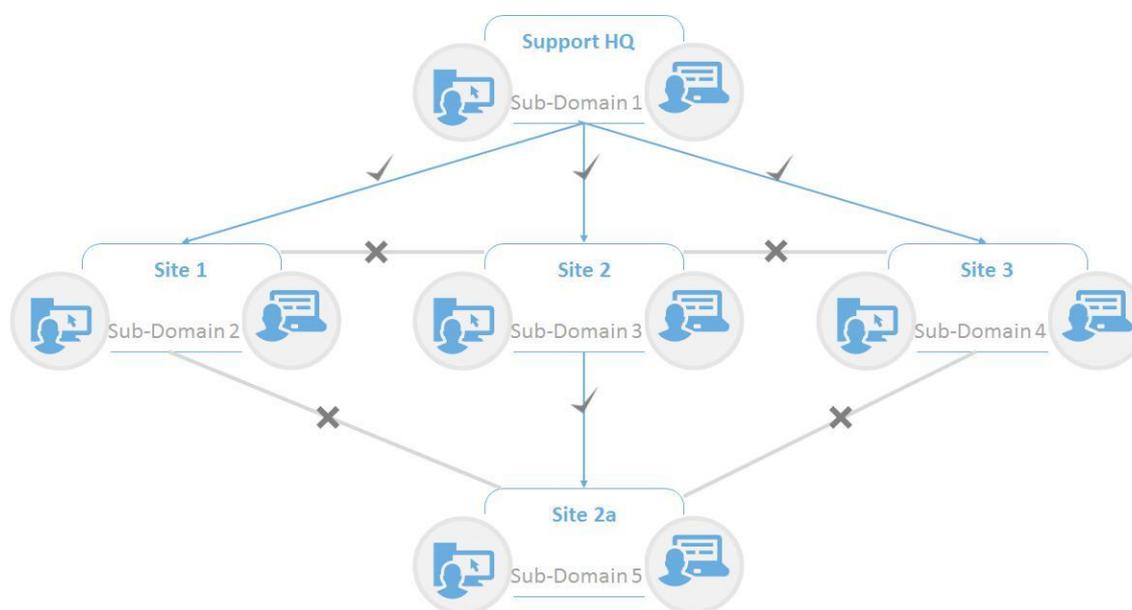
In this example, each sub-domain reflects a physical site that needs to be supported from the same **WebConnect** service located at Support HQ.

The Support HQ can set up a **WebConnect** account for their own **Guests** and this allows a connection path to the inherited **Hosts** in any child sub-domain

without switching to a different **WebConnect** profile in the **Guest** application. The architecture is designed to improve the connection process and management of large, dispersed enterprise environments.

Parent domains inherit **Hosts** from each child domain that is created. For example, the **Guests** from Site 2 can connect to the **Hosts** in the child domain called Site 2a, but they cannot connect to the **Hosts** in Site 1 or Site 3. **Guests** from Site2a will not be able to connect to **Hosts** in Site2. **Guests** in Site 1 and Site 3 can only connect to **Hosts** in their respective domains or any sub-domains that are created in their respective domains at a later stage.

To create subdomains, make sure that you log in to the **Connection Manager** with the site admin account. From here, the **Add Subdomain Account** option can be used to create the subdomain and the domain admin account for the new subdomain. Once a subdomain is created, click on the new subdomain button to either set up a new subdomain or create user accounts for the current subdomain.

Use the navigation path to ensure you edit the details in the correct subdomain and to switch between subdomains. The user accounts are the accounts that should be used within the **Impero** applications. Site admin and domain admin accounts are not valid accounts for use within the **Impero** applications and should only be used for **WebConnect** administration and subdomain management.

Domain administrator

If you are a domain administrator, you will probably not be sitting at the server machine where the site administrator installed the **Connection Manager**. This means that to log on to the **Connection Manager**, specify the right IP address or DNS name (Example: http:// CM.Company.com/ImperoCM) for the **Connection Manager** in the address field of the browser. Log on the

Connection Manager as admin (**Account**: admin, **Password**: admin, **Domain**: WebConnect). When you log in the **Connection Manager** as (domain) admin, the following page is displayed:
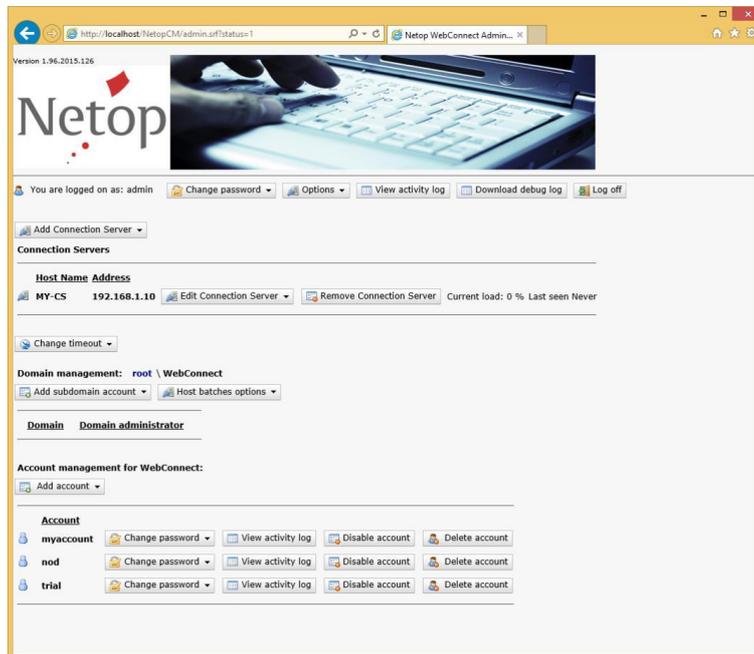
NOTE: When you log on you see that two more accounts with different rights are created in addition to the admin account. These are trial (Password: **trial**. Domain: **WebConnect**) and myaccount (Password: **myaccount**. Domain: **WebConnect**). If you have a **Netop OnDemand** license, you also see a nod account (Password: **nod**. Domain: **WebConnect**).

1. Click on the **Change password** tab, enter the new password and confirm it.

2. Click on the **Change** button for the change to take effect.

3. Click on **Change timeout** and enter the number of seconds for **Timeout for qualifiers in seconds** in the **HST** and **NOD** fields (**HST** for regular **Impero Host** and **NOD** for **Impero OnDemand Host**.)

When you browse for **Hosts** in the **Guest** and the **Connection Manager**, the **Hosts** are only displayed in the list of **WebConnect Hosts** if the **Hosts** polled the **Connection Manager** within the number of seconds specified in the **Timeout for qualifiers in seconds** fields in the **Connection Manager**. This means that a **Host** remains in the database for the specified number of seconds, after which it becomes inactive.

4. Click on the **Change** button for the change to take effect

5. You are now ready to create **WebConnect** accounts within the domain that you logged on to.

    a. To create a new account, click on **Add account** and make the following settings:

    b. In the **Account** field, enter an account name.

    c. In the **Password** field, enter a password for the account, and repeat it. You can change the password for the account later by clicking the **Change password** button for the account in the **Accounts Management** list. If necessary, you can also disable an account by clicking on the **Disable account** button for the account in the **Accounts Management** list.

6. Click on the **Add** button to add the account to the **Accounts Management**

list.

NOTE: You can also disable or delete any account that you created by clicking on the **Disable** button or the **Delete** button for the account in the list.

Hosts

Hosts are registered automatically in the **Connection Manager** when you specify the correct **Connection Manager** URL and credentials (account, password, domain) in the **Setup Wizard** of the **Hosts**.

However, you can log on to the **Connection Manager** using the account used by the **Host** to change the password or view the activity log for that account. You can edit the **Polling interval** for the **Hosts** here if you click on the **Edit Host** button and edit the respective fields in the drop-down.
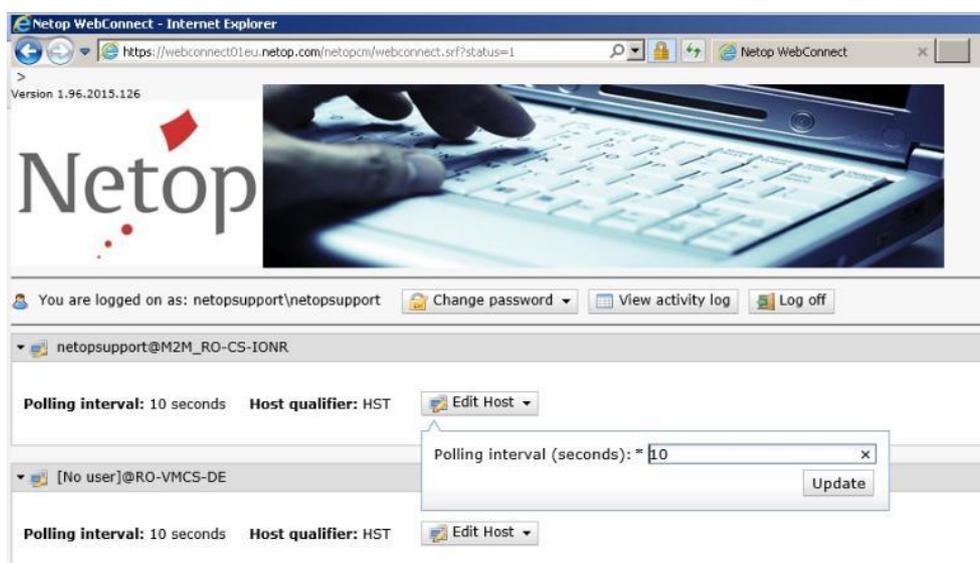
2.2.1 Manage Guest access to Hosts in WebConnect

When a **Guest** user is no longer allowed to access the **Host** computers the user had access to through the **WebConnect** service, for example, because the user is no longer on the project or no longer within the company, the user's **Guest** account can be disabled so that **WebConnect** no longer authenticates the user.

2.2.2 Manage Security Servers

For compatibility between **WebConnect** and **Security Server,** you can define which **Security Servers** the **Hosts** use when connecting via **WebConnect**. The **Security Server** provides enterprises with centralized identity management, granular access permissions, and accountability for their remote access solution helping to ensure that tough industry compliance regulations are met.

Hosts can be configured to authenticate against any number of **Security Servers**, and these are typically identified on the **Host** using the **IP Broadcast List**. When connecting to the **Hosts** using **WebConnect**, the required **Security Servers** can be defined using the **Connection Manager** on a per-domain basis.

This list is used to inform the **Hosts** which **Security Servers** to use to authenticate the connecting **Guest**. Using this centralized approach allows administrators easy web-based access to define which **Security Servers** to use within the enterprise.

Hosts require a UDP connection to the **Security Servers** and the locally defined **IP Broadcast List** is unrequired.

To define new **Security Servers**, make sure that you are logged on the **Connection Manager** with a **Domain Admin** account.
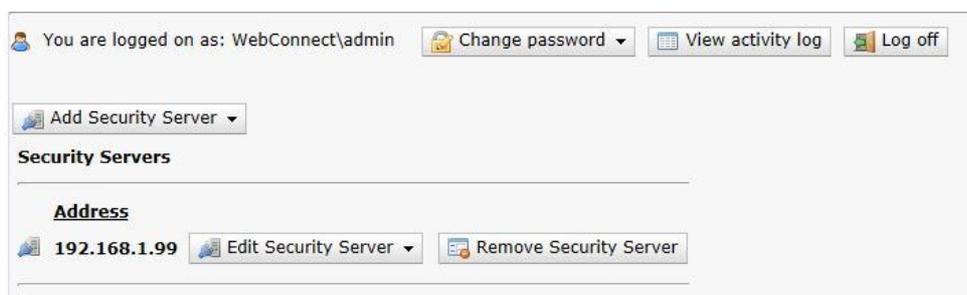
2.3 Connection Manager Activity log

Event logging records all activity and logon attempts in the **Connection Manager** activity log and thus provides very useful proof and documentation for instance in case of attacks or errors.

If you click on **View activity log** in the **Connection Manager**, the activity log is displayed.

NOTE: If you are logged on to the **Connection Manager** as an administrator, you can view the activity log for the administrator account, or you can view the activity log for each of the accounts in the **Accounts** list.

In the activity log, all events are logged with the type, a description and the time of the event.

Event types	
Information	
Log Alert	
Error	
Fatal Error	
Security Alert	

You can delete the content of the activity log if you click on the **Clear log** button at the bottom of the window. Also, you can download the activity log if you click on the **Download log** button at the bottom of the window.

Refer to the Impero Connect User's Guide for more information on event logging.

2.4 Connection Manager debugging options

The debug settings can be accessed from the **Options** button in the **Connection Manager** when you are logged in with the root Admin account.

NOTE: We recommend that you enable these settings only when advised by a Impero support representative.
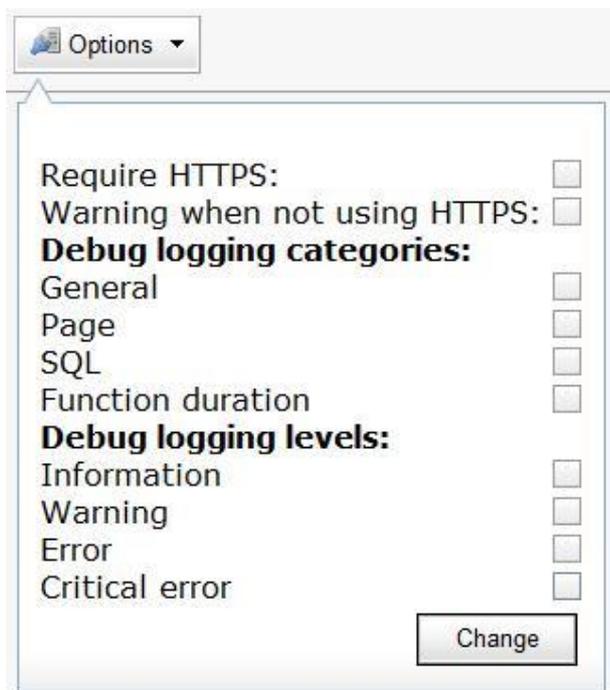
The individual debugging options are briefly described below:

Option	Description
Debugging logging categories	
General	Common events not associated with other categories.
Page	Errors that prevent web pages from displaying correctly.
SQL	Errors relating to SQL queries.
Function duration	Displays the duration of each function call within the application.
Debugging logging levels	
Information	Informative events unrelated to any specific errors.
Warning	Events that lead to unwanted behavior unrelated to any specific errors.
Error	Events triggered by errors within the application.
Critical error	Error events that cause the application to become inoperable.

Logging is effective when any of the options are enabled. When you want to retrieve the debug information, click on the **Download debug log** button and save the **.csv** file.

To reduce the database size, a cleanup script runs automatically and helps ensure that the debug data is only maintained for up to 30 days.

2.5 Optional tools

2.5.1 Activate the script for tidying up the log

Activate the installed script to tidy up the log by manually starting the SQL Server Agent service and changing the startup type to automatic:

1. In Windows Server, go to **Start** > **Administrative Tools** > **Services**. The **Services** window is displayed.

2. In the right pane, right-click on **SQL Server Agen**t. The **SQL Server Agent Properties** window is displayed.

3. In the **General** tab, from the **Startup type** drop-down, select **Automatic**.
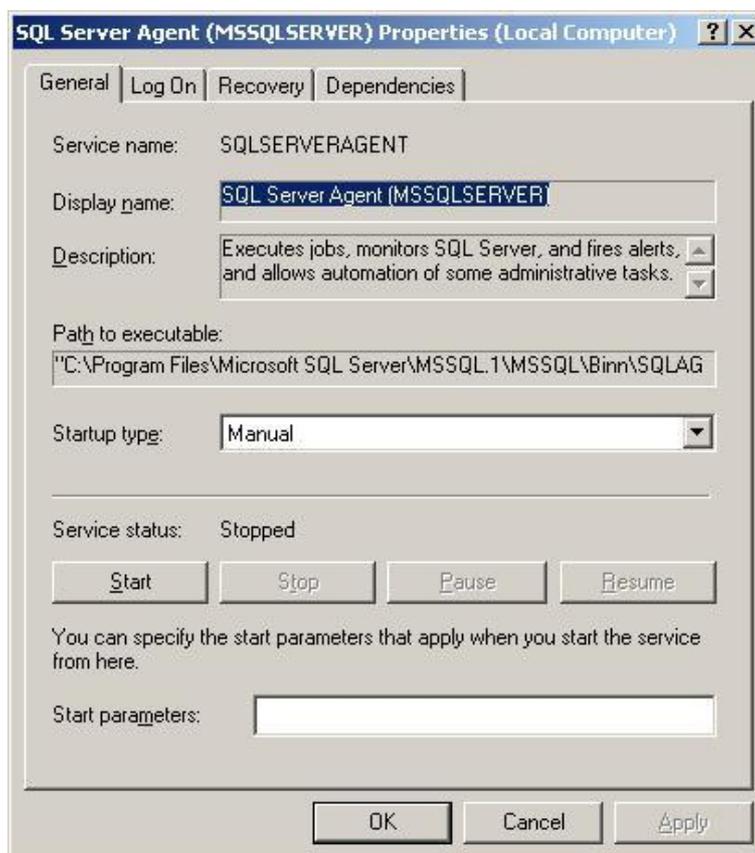
4. Click on the **Start** button to start the service.

5. Click on **OK** to close the window.

NOTE: This applies only to SQL Server. If you are running SQL Server Express, the SQL Server Agent is not available.

2.5.2 Customize the jobs for tidying up the tables

If the SQL Server is installed on a different machine than the **Connection Manager**, the existing jobs from Microsoft SQL Server should be edited and it is necessary for a script to be copied and edited from the **Connection Manager** machine.

To copy the scripts, proceed as follows:

1. Go to `C:\Program Files\Danware Data\Impero WebConnect\Wizard\`.

2. Copy the „`RenameArchive.vbs`" file to the SQL Server machine, in a folder of your choice.

To edit the script, proceed as follows:

1. Edit the „`RenameArchive.vbs`" from the SQL Server machine (the one copied in the above steps).

2. Find the following line:

   ```
   strDestination =
   WshShell.ExpandEnvironmentStrings("%ALLUSERSPROFILE%") &
   "\Application Data\Danware Data\ConnectionService\Logs\"
   & XmlFileName &    strDate & ".xml".
   ```

3. Replace the

   ```
   WshShell.ExpandEnvironmentStrings("%ALLUSERSPROFILE%") &
   ```

```
"\Application Data\Danware Data\ConnectionService\Logs\"
```

line with the path where you want to save the logs.

Edit the SQL Jobs

This procedure customizes the existing jobs to use the newly copied script from the previous step.

1. Start the Microsoft SQL Server Management Studio.

2. Go to **SQL Server Agent** > **Jobs**.

3. Right-click on **Active Tickets Archiving ImperoCM** ("ImperoCM" is a custom field, which mirrors the database name used by the **Connection Manager**).

4. Select **Properties**.

5. Go to **Job step** 4 in the list.

6.To edit the file, double click on it.
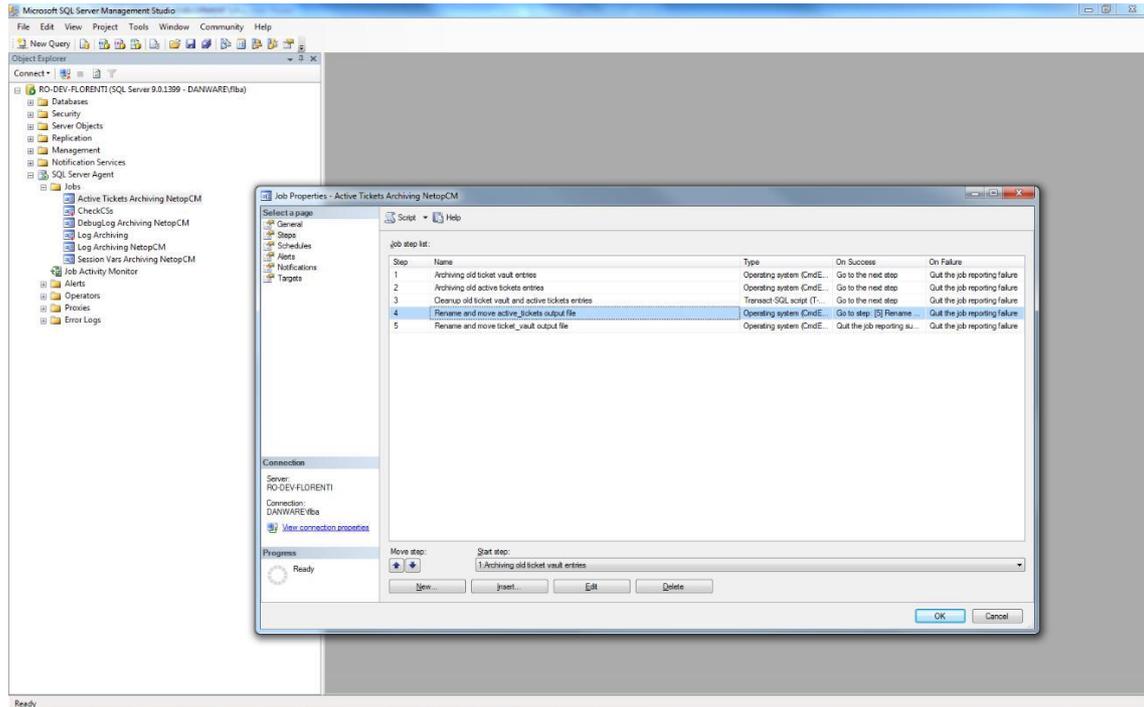
7.Change the `C:\Program Files\Danware Data\Impero WebConnect\Wizard\RenameArchive.vbs` path to the full path to where you copied the script.
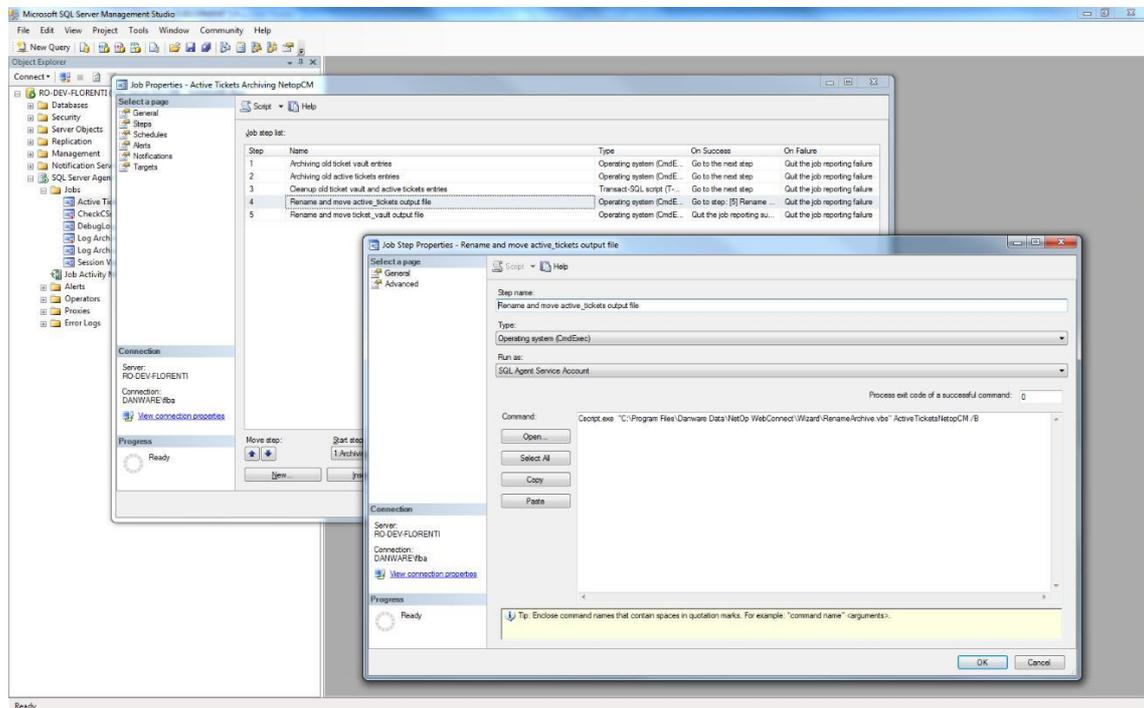
8.Repeat for **Job Step 6** („Rename and move…").

9.Repeat the same steps for all jobs in the SQL Server Agent Jobs (**Active Tickets Archiving**, **DebugLog Archiving**, **Log Archiving** and **Session Vars Archiving**).

NOTE: This applies only to SQL Server. If you are running SQL Server Express, the SQL Server Agent is not available.

2.5.3 Set up monitoring of Connection Servers

A **Connection Server** can stop responding for various reasons. To receive notifications by email about non-responsive **Connection Servers**, set up monitoring of **Connection Servers** in SQL Server Management Studio.
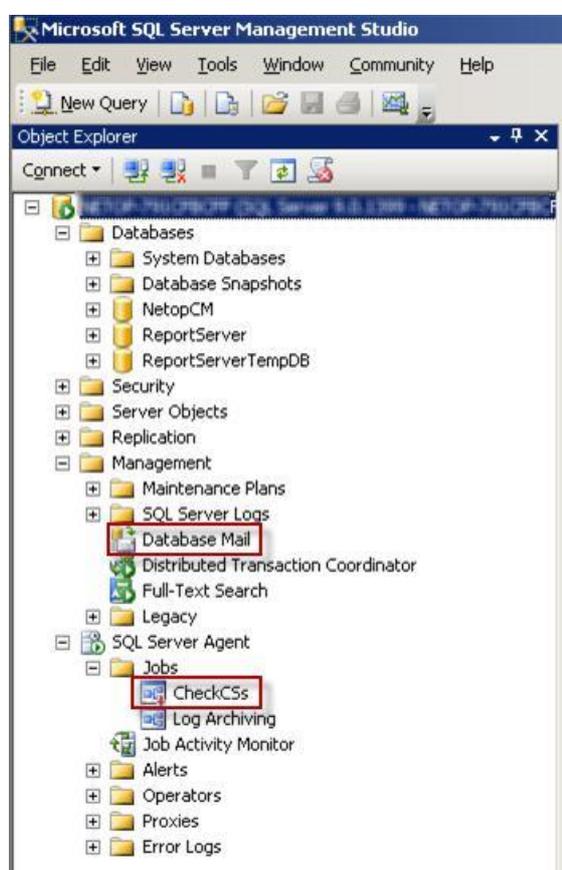
To set up the **Database Mail**, proceed as follows:

1. In the left pane of **SQL Server Management Studio**, go to **Management.**

2. Right-click on **Database Mail.**

3. Select **Configure Database Mail**. The **Database Mail Configuration Wizard** starts.

4. Click on **Next**. The **Select Configuration Task** page is displayed.

5. Select **Set up Database Mail** by performing the following tasks.

6. Click on **Next**. The **New Profile** page is displayed.

7. In the **Profile Name** field, enter a profile name.

8. In the **Description** field, specify a description for the mail profile for monitoring the **Connection Server**.

9. To add an SMTP account, click on the **Add button**. The **Add Account to Profile** dialog box is displayed.

10. Click on **New Account**. The **New Database Mail Account** dialog box is displayed.

11. In the **Account name** field, enter an account name.

12. To specify an **Outgoing Mail Server (SMTP)** enter the email address, display name, and the server name in the corresponding fields below.

   Tip: We recommend you enter the IP address of the Outgoing Mail Server in the **Server name** field.

13. Select the authentication relevant for your SMTP server.

14. Click on **OK**. The account is now listed in the **SMTP accounts** list on the **New Profile** page.

15. Click on **Next**. The **Manage Profile Security** page is displayed.

16. Select the **Public** checkbox next to the profile you created.

17. Click on **Next**.

18. In the following wizard pages click on **Next** to finish the mail setup.

19. Click on **Close**.

To edit the SQL Server Agent, proceed as follows:

1. In the left pane of **SQL Server Management Studio**, go to **SQL Server Agent** > **Jobs**.

2.   Right-click on **CheckCSs.**

3.   Select **Properties**. The **Job Properties** dialog box is displayed.

4. In the left pane, click on **Steps**.

5. In the left pane, from the **Job step** list select the relevant step.

6. Click on **Edit**.

7. In the lower right pane, edit the following information:

a. Set **@parm_profile_name** = [The profile name you chose during the Database Mail setup].

b.   Set **@parm_recipients** = [The email address you specified for Outgoing Mail Server during Database Mail setup].

8. Click on **OK.**

9. Close **SQL Server Management Studio**.

NOTE: This applies to SQL Server only. If you are running SQL Server Express, Database Mail and SQL Server Agent are not available.

3. Update Connection Manager

When updating the **Connection Manager**, we recommend you uninstall the previous version.

Uninstalling the **Connection Manager** does not impact your database configuration.

4 Connection Server setup

The **Connection Server** routes the traffic between a **Impero Host** and a **Impero Guest**.

Install the Connection Server

To install the **Connection Server**, proceed as follows:

1. Copy the installation file (**ImperoConnectionServer_uk.msi**) to the machine on which you want to install the **Connection Server**.

2. Execute the installation file.

3. Follow the onscreen instructions.

4. Select **Typical** installation. Leave all the settings as they are.

Set up the Connection Server

After the installation, run the **Setup Wizard** and follow the wizard onscreen instructions. Make sure that you set up the **Connection Server** for **WebConnect**.

To set up the **Connection Server** for **WebConnect**, proceed as follows:

1. Specify a password that is required from all the Guests to log on to the Host part of the **Connection Server**.

2. Enter the URL address of the **Connection Manager**, for example, http:// webconnect.provider.com/Imperocm.

3. Enter the passphrase you specified in the **Connection Manager**. This is used for the **Connection Manager** to accept communication with the **Connection Server**.

Communication profile and port number

Configure the **Connection Servers** to use the same protocol and port numbers as specified in the **Connection Manager**:

1. Click on **Tools** > **Communication Profiles**.

2. Enable the checkbox next to each relevant communication profile. For example, if you use TCP with automatic HTTP fallback, enable both the TCP and HTTP.

3. If you change the default port numbers for HTTP and/or TCP in the **Connection Manager**, select the relevant communication profiles.

4. Click on **Advanced.** Make sure that the **Use default port numbers** checkbox is not selected.

5. Enter the same port number as specified in the **Connection Manager**.

6. Click on **OK.**

7. Click on **OK**.

5 Configuration of Impero Guest and Host for WebConnect

After the installation of the **Impero Guest** and **Host** for the first time, the **Setup Wizard** starts automatically. Otherwise, you can run the wizard from the **Tools** menu of the **Impero Guest** and **Host**.

During the configuration, select to use **WebConnect**.
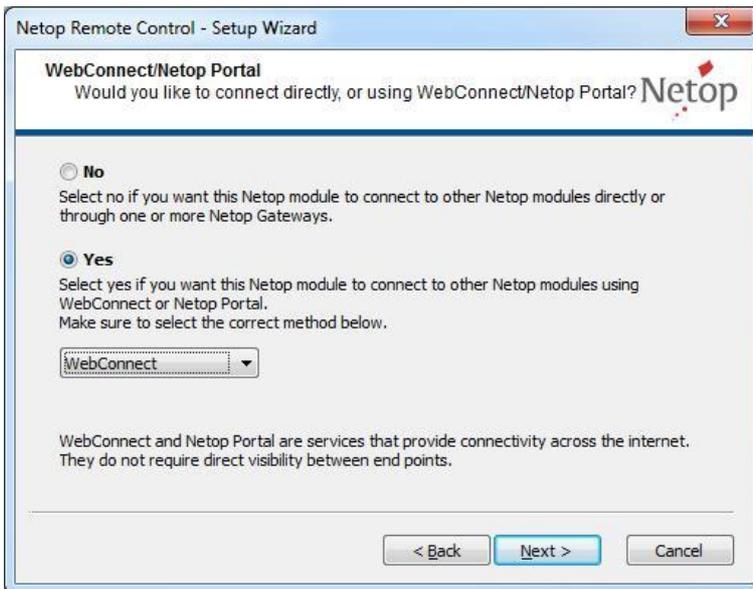
You also need to enter the URL address of the **WebConnect** service and logon credentials for your **Connection Manager** account.
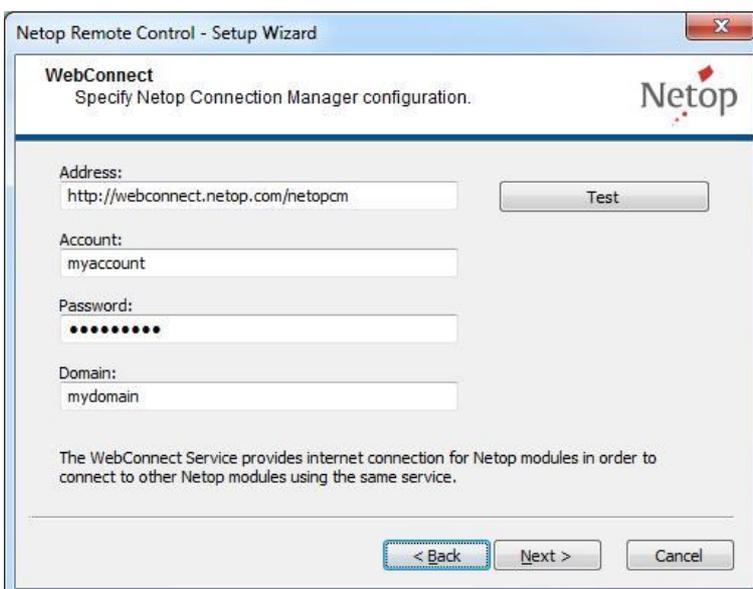
NOTE: The account named "**trial**" can only be used by the Impero **Guests** and **Hosts** with trial licenses. **Guests** and **Hosts** with trial licenses cannot use other accounts. Non-trial **Guests** and **Hosts** cannot use the account named "**trial**".

Refer to the **Setup Wizard** and **WebConnect** sections of the Impero Connect User's Guide for more information on how to configure the Impero **Guests** and **Hosts**.

Impero OnDemand Guest Ex and Host

If you intend to run **Impero OnDemand**, you require an "**extended**" license for your **Guest**. You configure the extended **Impero Guest** the same way as a regular **Impero Guest** using the **Setup Wizard**.

The procedure is, however, slightly different with the **OnDemand Host**. You create the **OnDemand Host** using **Impero OnDemand Pack'n Deploy**. The tool allows you to do this in various ways. You can create the **OnDemand Host** by running the configuration wizard, by entering the necessary information using the ribbon bar settings, or by setting up the necessary attributes in the attributes pane.

You have the option to specify the **Connection Manager URL**, or you can allow the end-user to enter the URL address at run-time. You can specify the credentials to apply and specify a ticket that is used as a display name in the **Connection Manager** list of **Hosts**. You can also allow the end-user to specify the ticket at run-time.

Refer to the Impero OnDemand Pack'n Deploy Guide and the Impero OnDemand Quick Guide for more information about Impero **OnDemand**

6 Metrics

Service capacity

The upper limit of concurrent **Guest**-**Host** sessions is 100 per **Connection Server**. The actual capacity depends on client bandwidth and the available bandwidth for the **Connection Server**. Sufficient screen transfer speed for clients is a subjective measure and very hard to qualify.

Client poll cost

Each client (**Host**) poll which is used to maintain **Host** status as active and ready for contact involves **Connection Manager** traffic cost less than 600 bytes in each direction within approx. 100 msec. equivalent to an average of approx. 1 kbps per **Host** with the default polling interval of 10 sec.

Database

- Activity log: Maximum 300 bytes per entry
- Host Information: Maximum 200 bytes per Host