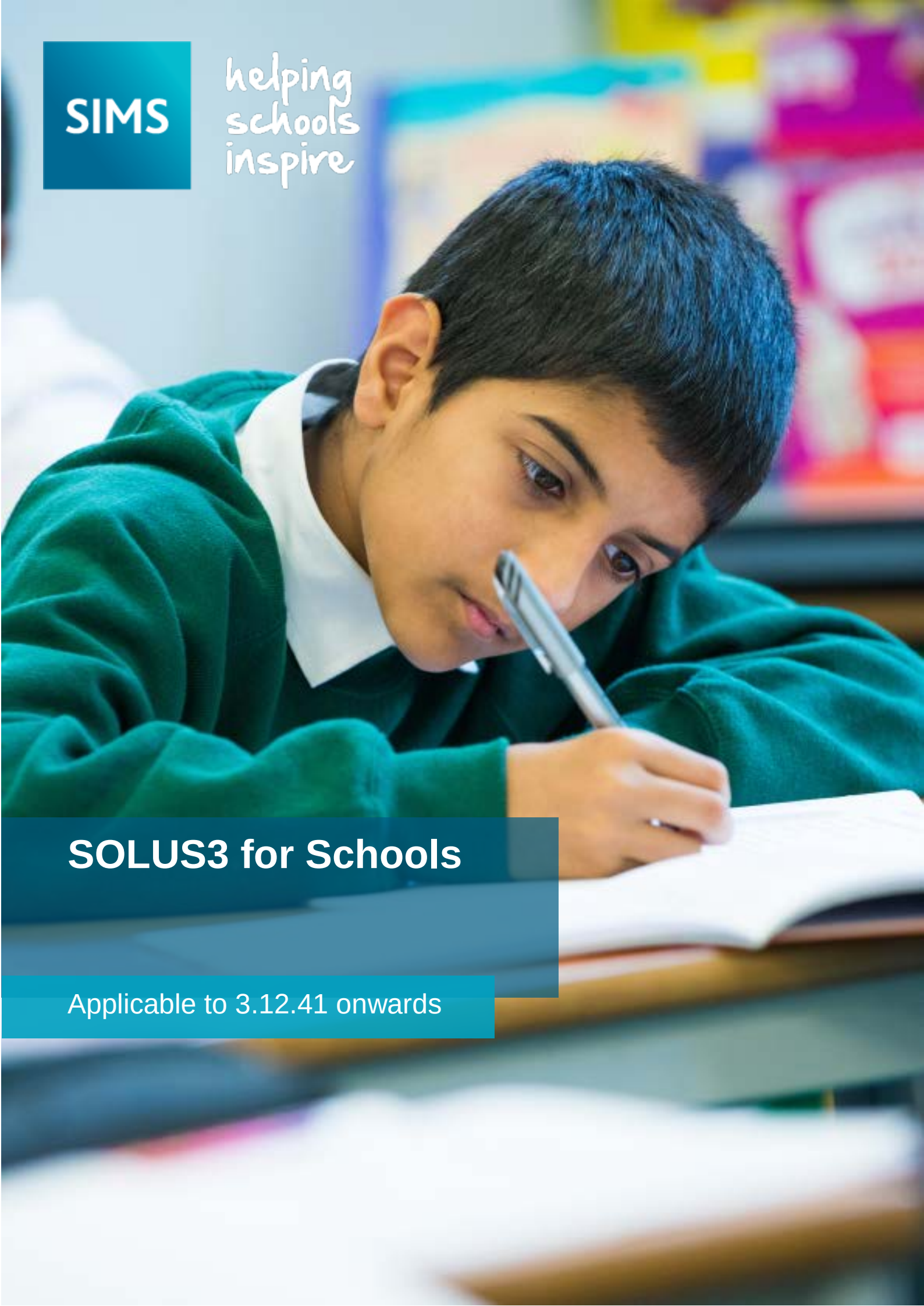


SIMS

helping schools inspire

SOLUS3 for Schools

Applicable to 3.12.41 onwards

Revision History

Version	Change Description	Date
3.12.41 - 1.0	Initial release.	24/10/2017

Capita Doc Ref: SOLUSSchool31243/HBK/241017

Providing Feedback on Documentation

We always welcome comments and feedback on the quality of our documentation including online help files and handbooks. If you have any comments, feedback or suggestions regarding the module help file, this handbook (PDF file) or any other aspect of our documentation, please email:

publications@capita.co.uk

Please ensure that you include the module name, version and aspect of documentation on which you are commenting.

CAPITA

Capita SIMS, Franklin Court, Priory Business Park, Cardington, Bedfordshire MK44 3JZ
Tel: 01234 838080 Fax: 01234 832036 Email: info@capita-sims.co.uk Web: www.capita-sims.co.uk

Contents

01 | Overview of SOLUS3

Introduction

What is SOLUS3?

SOLUS3 (SIMS Online Upgrade Service) is the latest Capita SIMS upgrade technology. SOLUS3 improves the efficiency of your SIMS, Discover and FMS upgrades and makes the installation of new SIMS, Discover and FMS clients easier to manage. One central console enables you to manage all of the server and workstation upgrades, enabling you to track the complete upgrade process.

How does SOLUS3 Work?

SOLUS3 is an enhancement to the SOLUS2 online upgrade technology, and fundamentally changes the upgrade process from a 'pull' technology to a 'push' technology. Workstations no longer pull their upgrades from the server; their upgrades are pushed out.

SOLUS3 requires an installation by an experienced SIMS engineer before it can be used. Once installed and configured, the SOLUS3 upgrade process starts with the school's software authoriser (Capita or their support team), making software available to the school's SOLUS3 system. The upgrade software is downloaded and the school chooses when to apply the upgrade.

The upgrade process takes responsibility for upgrading all SIMS, Discover and FMS server components, as well as any workstations that have been configured with workstation agents.

When configuring SOLUS3, schools can choose not to deploy SOLUS3 workstation agents, but instead opt to auto-extract the workstation/client files to a folder that can then be used to update manually a SOLUS1/SOLUS2 setups directory. This route does not provide any of the workstation upgrade benefits.

What are the Benefits of Moving to SOLUS3?

SOLUS3:

- enables SIMS upgrades to be fully automated on a specific day of the week.
- can deliver workstation upgrades outside of a main SIMS release, meaning important client updates can be delivered without having to wait for the next main release (this requires SOLUS3 agents).

- can be used to install new SIMS and FMS workstations from a central management console (this requires SOLUS3 agents).
- can be used to install Discover and Discover workstations from a central management console.
- can send email alert confirmations after an upgrade.
- can manage any future infrastructure updates, such as .NET Framework.

Can I use a CD to Upgrade SIMS?

For the foreseeable future, SIMS will continue to create SOLUS1 ISO images for SIMS, Discover and FMS. This option is predominantly designed for teams that centrally host SIMS or for teams that are licensed to use SIMS test environments.

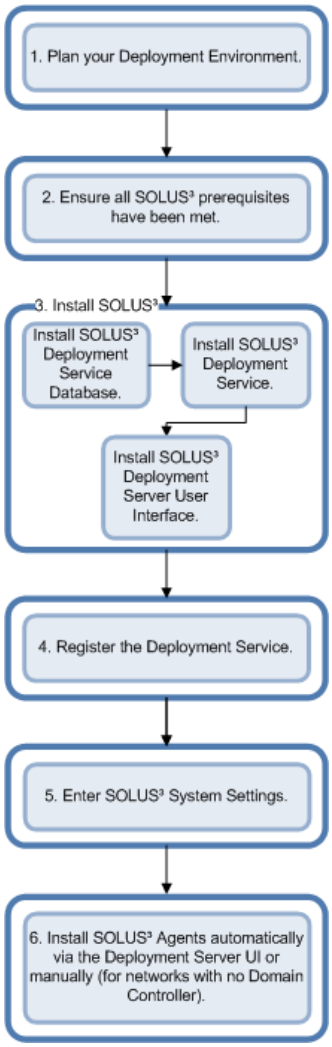
What's New in this Release?

- SOLUS3 now supports the use of Microsoft SQL Server 2016.
- It is now possible to determine which client and school targets will receive updates first by specifying individual deployment priorities via **Environment | Targets | Clients**.
- Packages that are over a year old (excluding infrastructure packages) can be deleted from the repository to maximise available space via **Settings | SOLUS3 | SOLUS | Clean Repository**.

Installing and Using SOLUS3 - Process Flow Diagram

This process flow diagram summarises the procedures that must be followed to install and configure SOLUS3.

These procedures must be completed by any Local Authority (LA), Regional Centre (RC), or school that hosts a Deployment Service.



Troubleshooting

Log Files

Log files can be useful for troubleshooting purposes. SOLUS3 creates the following log files:

- `ds_systemlog.txt`
- `ui_systemlog.txt`.

The default log file location depends on your version of Windows:

- `C:\Documents and Settings\All Users\Application Data\Capita\Solus3\Logs`
- `C:\ProgramData\Capita\Solus3\Logs`.

02 | Preparing for a SOLUS3 Installation

Introduction

Before installing the SOLUS3 components, ensure that your network environment, including firewalls, is configured appropriately, and that your software meets the minimum requirements. This chapter outlines the steps that should be completed to ensure that your network environment is configured properly and that the software you have meets the SOLUS3 minimum requirements.

SOLUS3 Installation Checklist

Complete	Description
❑	Ensure that Network Administrators and Deployment Managers have discussed and documented how they will configure the SOLUS3 DE.
❑	Microsoft .NET Framework 4.5.0 must be installed on the device hosting the Deployment Service (http://www.microsoft.com/en-gb/download/details.aspx?id=30653).
❑	Framework 4.0 must be installed on all devices in the Deployment Environment.
❑	One of the following must be installed on the device that will host the Deployment Service database: ▪ Microsoft SQL Server 2016 ▪ Microsoft SQL Server 2014 ▪ Microsoft SQL Server 2012.
❑	Windows Task Scheduler must be enabled on each device in the environment, including the computer hosting the Deployment Service.
❑	To run the SOLUS3 installers, you must log on to the device that will host the Deployment Service as a Domain Administrator.
❑	You must have write access to the MachineKeys folder on the Deployment Service device. For Windows Server 2008, 2008 R2 and 2012, this is located at `[Drive]:\ProgramData\Microsoft\Crypto\RSA`. For Windows Server 2003, this is located at `[Drive]:\Documents and Settings\all users\Application Data\Microsoft\Crypto\RSA\MachineKeys`.

Complete	Description
❑	The following ports must be open on the firewalls of all devices in the deployment environment: ▪ TCP port 52965 (this port can be changed when installing the Deployment Service) ▪ TCP port 52966 (this port can be changed when installing the Deployment Service) ▪ TCP port 8739.
❑	The following ports must be open on the firewalls of all devices in the Deployment Environment to enable browsing of the network (NetBios): ▪ TCP port 139 ▪ UDP port 138 ▪ UDP port 137.
❑	Windows Management Instrumentation (WMI) must be enabled on the firewalls of all devices in the Deployment Environment. For more information, please refer to the *Authorize WMI users and set permissions* Microsoft TechNet article (http://technet.microsoft.com/en-us/library/cc771551.aspx). If you are installing the SOLUS3 agents to devices manually, you do not need to enable WMI.
❑	A network share must be set up to host the Update Repository for SIMS update downloads. The Deployment Service must have write access to this network share.
❑	If you want SOLUS3 to create backups of your Capita SIMS databases before deploying updates, ensure that the SQL Servers have sufficient disk space to accommodate such backups.

More Information:
Enabling Windows Task Scheduler on page *10*
Ensuring Access to the MachineKeys Directory on page *10*
Configuring the Windows Firewall on page *7*
Step 2 – Enabling WMI Through the Windows Firewall on page *9*
Update Repository Requirements on page *6*

Update Repository Requirements

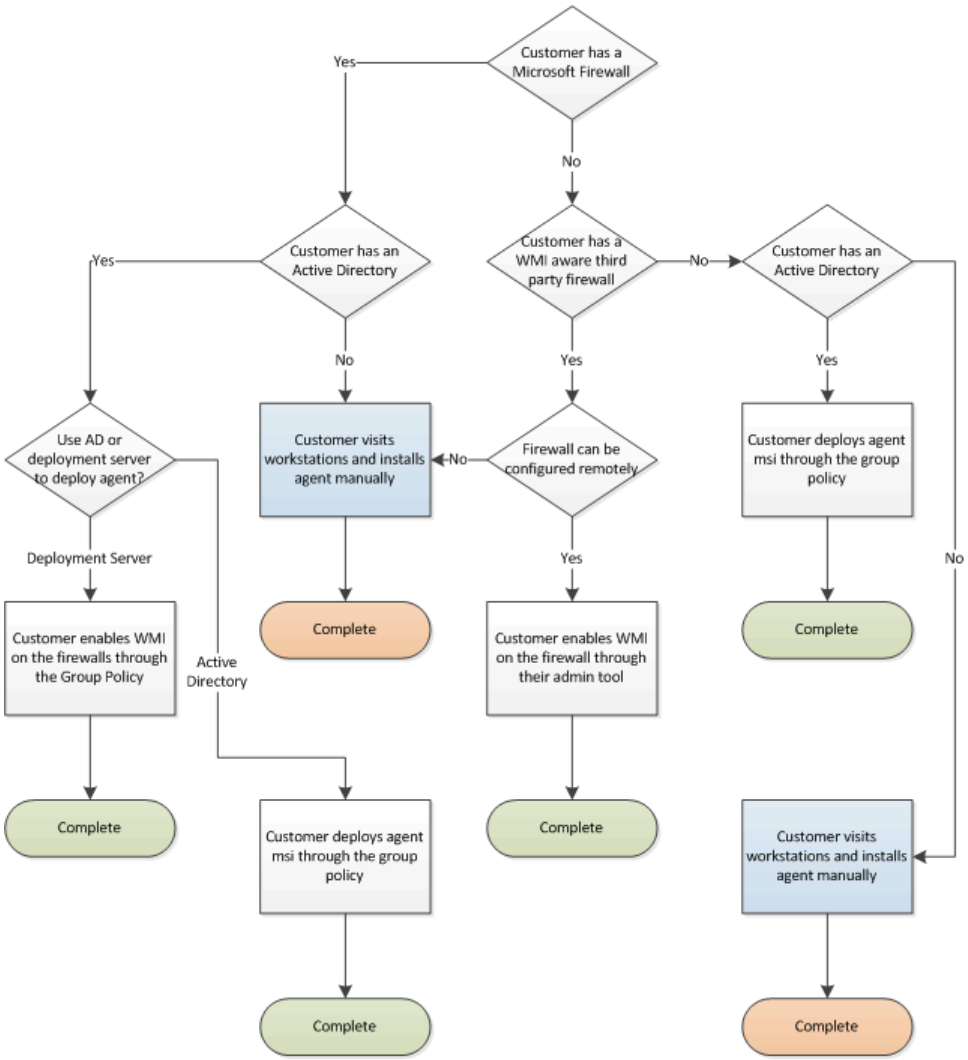
The Update Repository is a network share that hosts update files. The share can be hosted on any platform, as long as it can be written to by the Deployment Service.

NOTE: The share that will host the Update Repository should be set up before installing SOLUS3.

Configuring the Windows Firewall

Configuring Firewalls (Flowchart)

The following flowchart assists Network Administrators to plan the SOLUS installation and configuration. It shows the process of configuring the Deployment Environment in relation to your firewall and your Active Directory (AD) configurations.



Step 1 – Configuring the Windows Firewall for SOLUS3 Agent Communication

Ensure that the following firewall settings are applied before commencing configuration:

- Devices running the SOLUS3 agent must have the correct port open in the firewall.
- The server running the Deployment Service must have the correct port open in the firewall.
- Log in to Windows as a user with Administrator rights.

1. Load the Group Policy Editor.

For more information, refer to the *Deploying Windows Firewall Settings With Group Policy* Microsoft TechNet article (http://technet.microsoft.com/en-gb/library/bb490626.aspx).

2. Navigate to the Windows Firewall node. In the panel on the left-hand side, select **Computer Configuration |** (**Policies**) | **Administrative Templates | Network | Network Connections | Windows Firewall | Domain Profile**.

   IMPORTANT NOTE: *Ensure that all of the following Windows Firewall settings are accessed via the stated route only.*

3. Open the **Windows Firewall: Define inbound port exceptions** dialog.
   a. In the panel on the right-hand side, double-click **Windows Firewall: Define inbound port exceptions**.
   b. Select the **Enabled** radio button.
   c. In the **Options** panel, click the **Show** button to display the **Show Contents** dialog.
   d. Click the first empty **Value** field, and enter `52965:TCP:*:Enabled:SOLUS 3 Deployment Server`.
   e. Click the next empty **Value** field, and enter `52966:TCP:*:Enabled:SOLUS 3 Agent`.
   f. Click the next empty **Value** field, and enter `8739:TCP:*:Enabled:SOLUS 3 Agent Notifier UI`.
   g. Click the **OK** button.
   h. Click the **OK** button.

      NOTE: Setting Group Policy port exceptions disables local port exceptions, unless overridden in the Group Policy.

   i. In the panel on the right-hand side, double-click **Windows Firewall: Allow local port exceptions properties**.
   j. Select the **Enabled** radio button, and then click the **OK** button.
4. Open the **Windows Firewall: Allow inbound remote administration exception properties** dialog.
   a. In the panel on the right-hand side, double-click **Windows Firewall: Allow inbound remote administration exception**.
   b. Select the **Enabled** radio button.
   c. In the **Options** panel, enter an asterisk (*****) in the **Allow unsolicited incoming messages from these IP addresses** field.
   d. Click the **OK** button.
5. Open the **Windows Firewall: Define inbound program exceptions** dialog.
   a. In the panel on the right-hand side, double-click **Windows Firewall: Define inbound program exceptions**.
   b. In the **Options** panel, click the **Show** button to display the **Show Contents** dialog.

c. Click the first empty **Value** field, and enter `C:\Windows\System32\wbem\unsecapp.exe:Enabled:.NET Proxy for DCOM (WMI)`.

d. Click the **OK** button.

6. Open the **Windows Firewall: Allow inbound file and printer sharing exceptions** dialog.
   a. In the panel on the right-hand side, double-click **Windows Firewall: Allow inbound file and printer sharing exceptions**.
   b. Select the **Enabled** radio button.
   c. In the **Options** panel, enter an asterisk (*) in the **Allow unsolicited incoming messages from these IP addresses** field.
   d. Click the **OK** button.
7. Open the **Windows Firewall: Allow ICMP exceptions** dialog.
   a. In the panel on the right-hand side, double-click **Windows Firewall: Allow ICMP exceptions**.
   b. Select the **Enabled** radio button.
   c. In the **Options** panel, select the **Allow outbound source quench** and the **Allow inbound echo request** check box.
   d. Click the **OK** button.
8. Close the Group Policy Editor.

Step 2 – Enabling WMI Through the Windows Firewall

WMI (Windows Management Instrumentation) must be enabled for SOLUS3 to work properly.

Additional Resources:

Windows 7, Windows Server 2008, Windows 8 and Windows Server 2012 (http://msdn.microsoft.com/en-us/library/aa822854(v=VS.85).aspx)

Step 3 – Force a Group Policy Refresh

On the target computer (the device that you want to apply the group policy settings to), run `gpupdate` from the command prompt. This pushes the group policy changes made in steps 1 and 2 out to the device. For details on `gpupdate`, consult Microsoft TechNet (http://technet.microsoft.com/en-us/library/bb490983).

Additional Resources:

Windows Vista and later (http://msdn.microsoft.com/en-us/library/aa822854(v=VS.85).aspx)

Firewall Settings Additional Reading

SOLUS can run on a variety of Microsoft networks, which in turn can have a wide range of network configurations. It is therefore impossible to provide bespoke instructions on how to configure your firewalls to work with SOLUS. To assist you as far as possible when changing firewall settings, please note that the following ports and services must be available:

- WMI must be enabled
- Port 139 (TCP), 137 (UPD) and 138 (UPD) for browsing the network (NetBIOS) on all devices.
- Port 8739 (TCP) for the Agent Notifier UI.
- Port 52965 (TCP) for the Deployment Service.
- Port 52966 (TCP) for the Agent
- Some Domain Controllers require that port 389 (TCP) be opened for LDAP.

Additional Resources:

Configuring a Firewall for Domains and Trusts (http://support.microsoft.com/kb/179442)

Enabling Windows Task Scheduler

Ensure that the Windows Task Scheduler is running on all devices in the DE before installing SOLUS.

When an agent is installed automatically on a device, SOLUS may first need to install .NET Framework 4.0 (http://www.microsoft.com/en-gb/download/details.aspx?id=17851).

To do this successfully, the Windows Task Scheduler must be enabled on all devices in the DE. If the Task Scheduler is not running, this is usually because it has been disabled through a Group Policy, or it has failed to start due to an error, which can be investigated in the Windows Event Viewer.

Ensuring Access to the MachineKeys Directory

If administrators do not have full read and write rights to the `MachineKeys` directory on the Deployment Server, they will be unable to register the site with Capita SIMS. The following error is reported during the site registration process:

Unable to register site error. An error occurred saving the Deployment Service security keys, please contact your local support unit. Access is denied.

To prevent these errors from occurring during registration, carry out the following process.

9. On the computer that hosts the Deployment Service, show hidden files and folders. For more information, please refer to the advice from Microsoft (http://windows.microsoft.com/en-gb/windows/show-hidden-files).
10. Navigate to the RSA folder: `C:\ProgramData\Microsoft\Crypto\RSA`
11. In the RSA folder, right-click the `MachineKeys` folder and then select **Properties** from the pop-up menu to display the **MachineKeys Properties** dialog.
12. Select the **Security** tab.

13. Click the **Edit** button.
14. In the **Group or user names** panel, click the **Administrators** group.
15. In the **Permissions for Administrators** panel, select the **Full control** check box in the **Allow** column.
16. Click the **Apply** button and then click the **OK** button.
17. Click the **OK** button again to exit the **MachineKey Properties** dialog.
18. Attempt to register the establishment with the Capita SIMS servers again.

03 | Installing SOLUS3

Introduction

Installing the SOLUS3 Deployment Service requires the installation of three components:

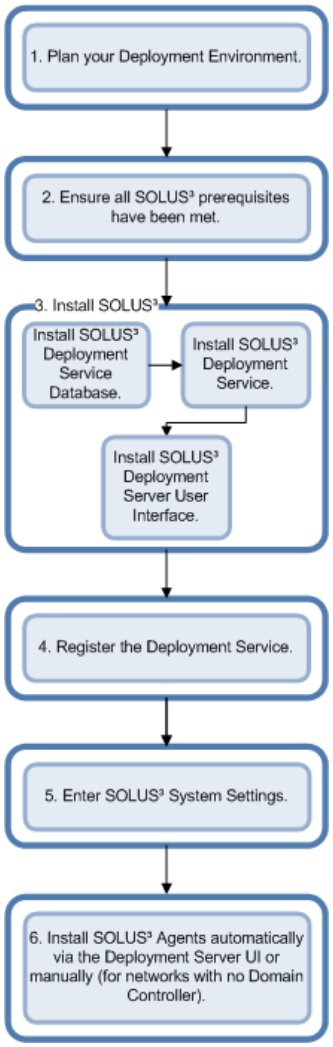
- the Deployment Server Database
- the Deployment Service (Windows Service)
- the Deployment Service User Interface (UI).

All of the components can be installed on the same computer if required, or on separate computers.

Installing and Using SOLUS3 - Process Flow Diagram

This process flow diagram summarises the procedures that must be followed to install and configure SOLUS3.

These procedures must be completed by any Local Authority (LA), Regional Centre (RC), or school that hosts a Deployment Service.



SOLUS3 Components Installation

The components must be installed in the following order:

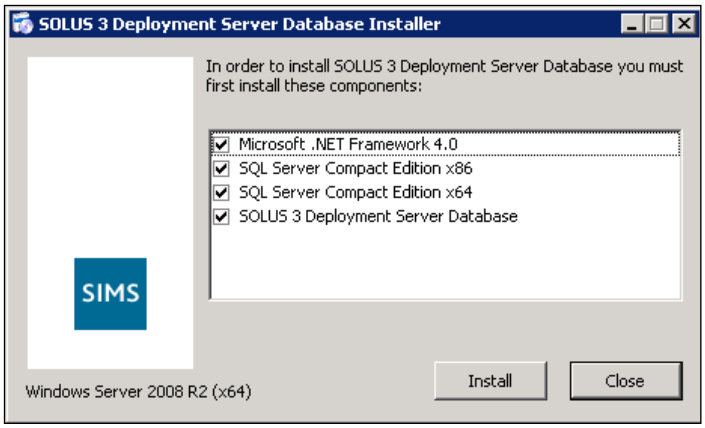
1. Installing the Deployment Service Database (please see *Installing the Deployment Server Database* on page *14*).
2. Installing the Deployment Service (please see *Installing the Deployment Service* on page *18*).
3. Installing the Deployment Server User Interface (please see *Installing the Deployment Server User Interface* on page *21*).

Installing the Deployment Server Database

The Deployment Server database is the underlying store for all SOLUS3 information. To install the Deployment Server database, you must log in to the device that will host the database as a Domain Administrator then complete the following procedure.

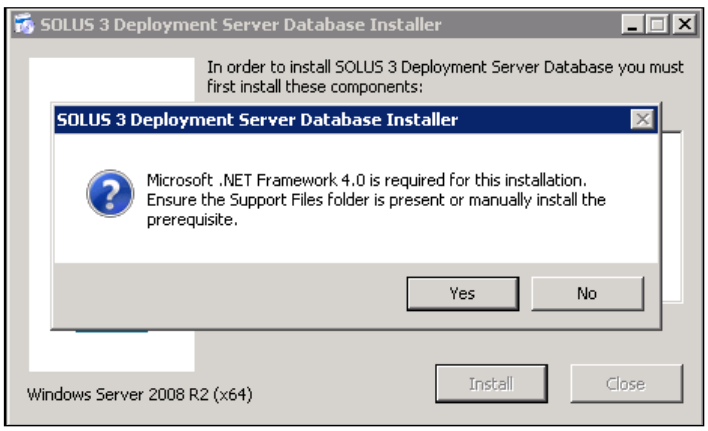
> ***WARNING:*** *If there is any pre-requisite software that has not been installed already, the installer will first run installation wizards for the required software. This might force a restart of your system. Ensure that you choose a time to run the installers when such a restart is acceptable.*

1. From the computer that will host the Deployment Server database, download SOLUS3<version_number>.ZIP from Capita SIMS to a folder of your choice.
2. Extract the content of the zip file. This produces a file named SOLUS3DeploymentServerDatabase.exe.
3. Double-click SOLUS3DeploymentServerDatabase.exe to display the **SOLUS 3 Deployment Server Database Installer**.

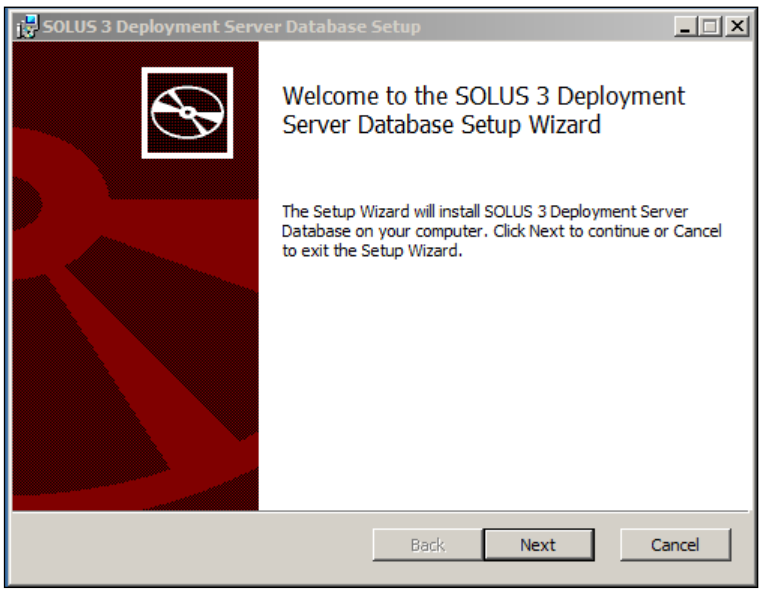


Microsoft .NET Framework 4.0, **SQL Server Compact Edition x86** and **SQL Server Compact Edition x64** are selected automatically if they are not already installed. **SOLUS Deployment Server Database** is selected automatically.

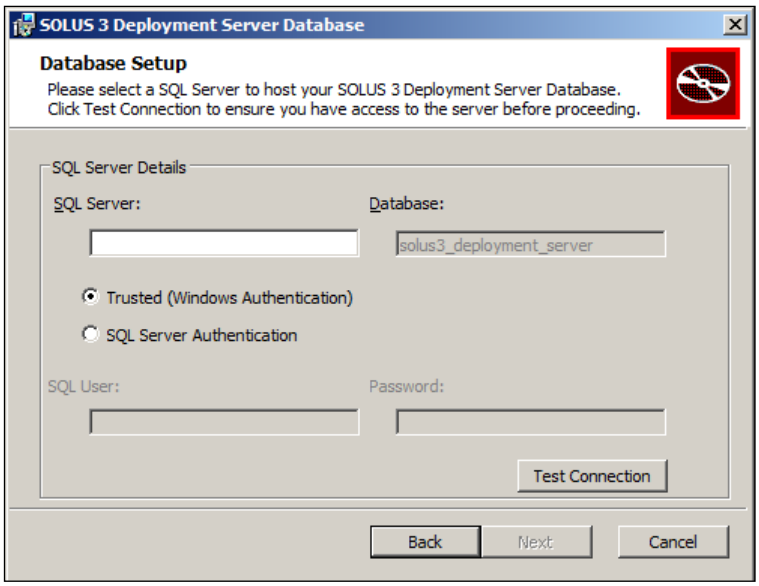
4. Click the **Install** button. Installing Microsoft .NET 4.0 requires a reboot.
5. Click the **Install** button to display the **SOLUS 3 Deployment Server Database Installer** dialog.



Click the **Yes** button to confirm the Support Files folder is present and to display the **Welcome to the SOLUS 3 Deployment Server Database Setup Wizard** page. If .NET Framework has not been installed, or the folder is not present, install .NET Framework 4.0 first.



6. Click the **Next** button to display the **End-User License Agreement** (EULA).
7. Select the **I accept the terms in the License Agreement** check box.
8. Click the **Next** button to display the **Database Setup** page.



9. In the **SQL Server** field, enter the server\instance for the Deployment Service database, e.g. `MS2012S\SIMS2K14`.

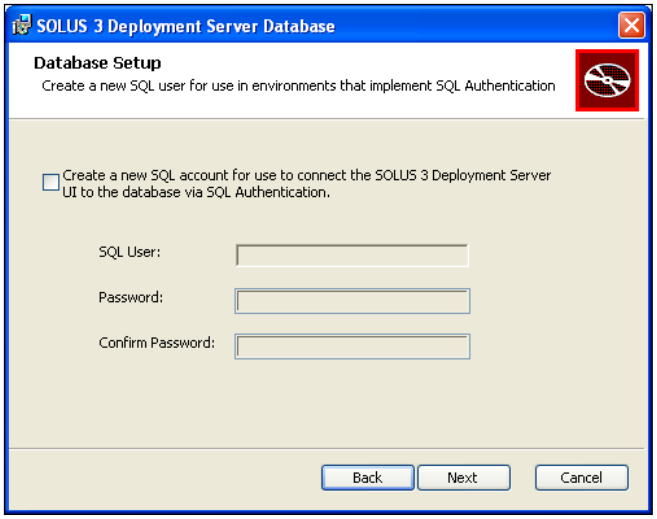
   The **Database** field defaults to `solus3_deployment_server` and cannot be changed.

10. Select the radio button required for your authentication method.

    If you select **SQL Server Authentication**, enter the Administrator credentials in the **SQL User** field and in the **Password** field.

11. Click the **Test Connection** button to test the connection and to display the **Database Information** dialog.
    - If the test is successful, click the **OK** button to close the dialog and return to the installer.
    - If the test is unsuccessful, ensure that the server details are correct and that the SQL server is online, and then click the **Test Connection** button again.

12. Click the **Next** button to display the **Database Setup** page.



> ***IMPORTANT NOTE:*** *To connect the SOLUS Deployment Server UI to the Deployment Database, it is possible to create a new SQL account. However, this is necessary only if you want to host the SOLUS Deployment Server UI (User Interface) on a separate computer from the* `solus3_deployment_server` *database.*

13. To create a new SQL account:
    a. Select the check box.
    b. Enter a name for the new **SQL User**.
    c. Enter and confirm a **Password** for the new SQL user.

    > ***IMPORTANT NOTE:*** *When you create a new SQL account, the password must conform to the SQL password requirements configured by the System Administrator. If the password does not meet these requirements, an error message is displayed.*

    d. Click the **Next** button.

    To skip the creation of a new SQL account:
    a. Deselect the relevant check box if necessary.
    b. Click the **Next** button.

14. On the **Ready to install SOLUS 3 Deployment Server Database** page, click the **Install** button.

    This starts the file installation, which you can monitor using the progress bar.

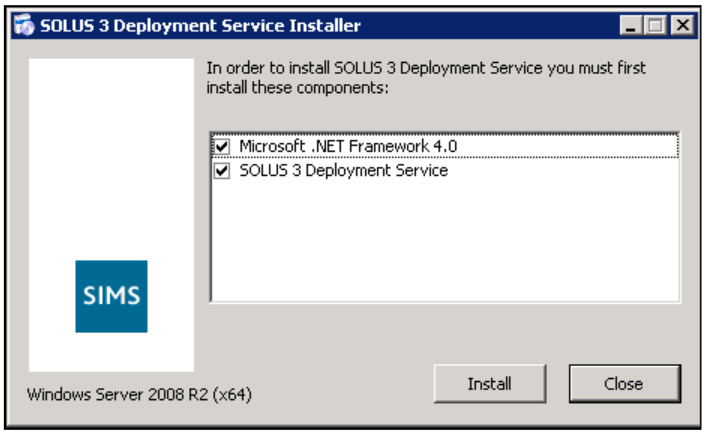
15. When the installation process is complete, the **Installation successful** dialog is displayed.
16. Click the **Finish** button, and then click the **OK** button.

Installing the Deployment Service

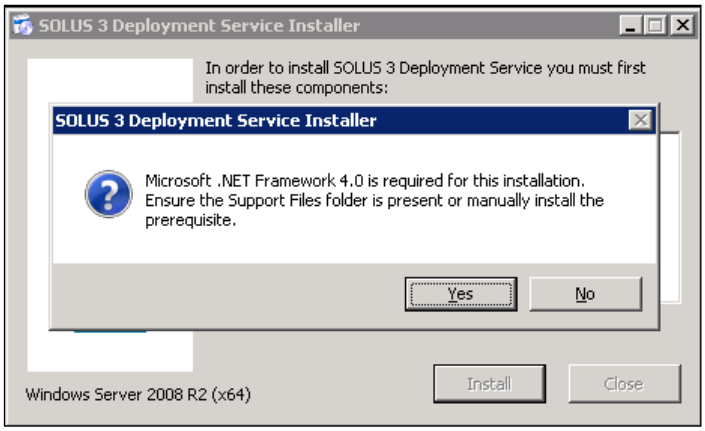
The SOLUS3 DS is a Windows service that supports all SOLUS3 operations. To install the service, you must log into the host machine as an Administrator and then complete the following procedure.

> ***WARNING:*** *If there is any pre-requisite software that has not been installed already, the installer will first run installation wizards for the required software. This can force a restart of your system. Ensure that you run the installers only when such a restart is acceptable.*

1. From the computer that will host the SOLUS3 Deployment Service, download `SOLUS3DeploymentService.exe` from Capita SIMS to a folder of your choice.
2. Double-click `SOLUS3DeploymentService.exe` to display the **SOLUS 3 Deployment Service Installer** setup wizard.



3. Click the **Install** button to display the **SOLUS 3 Deployment Service Installer** dialog.

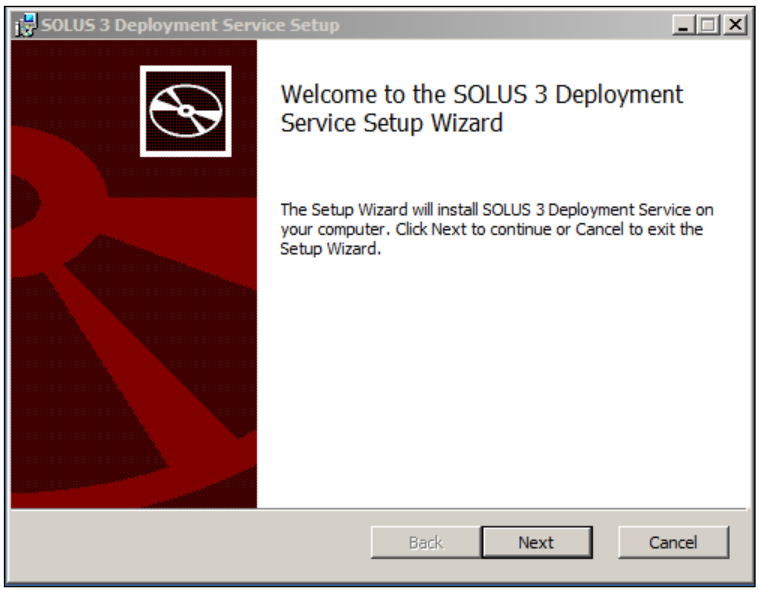


4. Click the **Yes** button to confirm the Support Files folder is present.

   The **Welcome to the SOLUS 3 Deployment Server Database Setup Wizard** page is displayed.

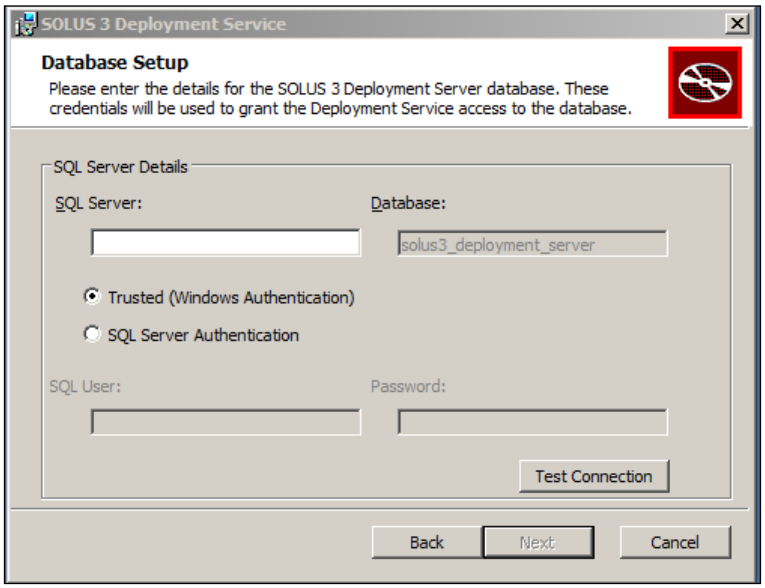
   If .NET Framework has not been installed, or the folder is not present, install .NET Framework 4.0 first.

5. Click the **Next** button to display the **End-User License Agreement** (EULA).



6. Select the **I accept the terms in the License Agreement** check box.

7. Click the **Next** button to display the **Database Setup** page.



8. In the **SQL Server** field, enter the server\instance for your Deployment Service database, e.g. `MS2012S\SIMS2K14`.

   The **Database** field defaults to `solus3_deployment_server` and cannot be changed.

9. Select the radio button required for your authentication method.

   If you select **SQL Server Authentication**, enter administrator credentials in the **SQL User field** and in the **Password** field.

10. Click the **Test Connection** button to test the connection, and to display the **Database Information** dialog.
    - If the test is successful, click the **OK** button to close the dialog and return to the installer.
    - If the test is unsuccessful, ensure that the server details are correct and that the SQL server is online, and then click the **Test Connection** button again.
11. Click the **Next** button to display the **Service Port** page.
12. If necessary, change the default **Deployment Service Port**.
13. Click the **Next** button to display the **.NET Framework v4.0** page.

    If required, locate the `.NET Framework v4.0` setup file.

14. Click the **Select** button, navigate to the location of the setup file, and then click **Select**.

> *NOTE: The location of the .NET Framework v4.5.0 setup file should already be entered as it is included in the support files directory of the files downloaded from Capita SIMS. If the location is already entered, do not change the location.*

15. Click the **Open** button to return to the setup wizard.

    If the **Setup File Path** is already selected, click the **Next** button to display the **Destination Folder** page.

16. Use the default installation location, or click the **Change** button to select a new installation destination.
17. Click the **Next** button to display the **Ready to install SOLUS 3 Deployment Service** page.
18. Click the **Install** button to start file installation.

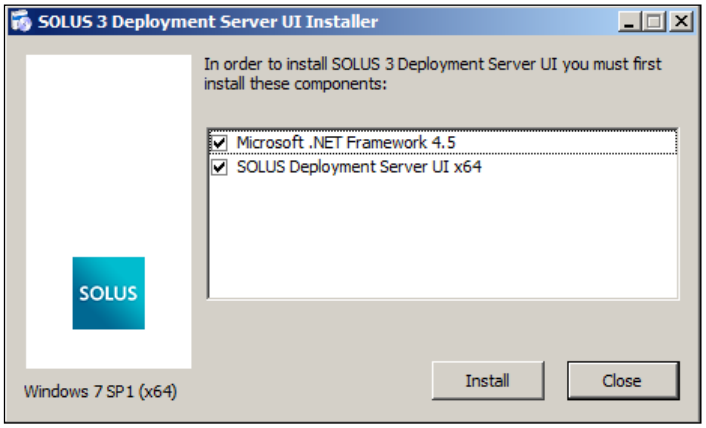
    You can monitor the installation process using the progress bar.
19. When the installation process is complete, the Installation successful dialog is displayed.
20. Click the **Finish** button, and then click the **OK** button.

Installing the Deployment Server User Interface

The SOLUS3 Deployment Server (DS) UI (User Interface) enables administrators to configure the Deployment Service and Deployment Environment. To install the Deployment Server UI, you must log on to the device that will host the user interface as an Administrator. You can then complete the following procedure.

> ***WARNING:*** *If there is any pre-requisite software that has not been installed already, the installer will first run installation wizards for the required software. This can force a restart of your system. Ensure that you run the installers only when such a restart is acceptable.*

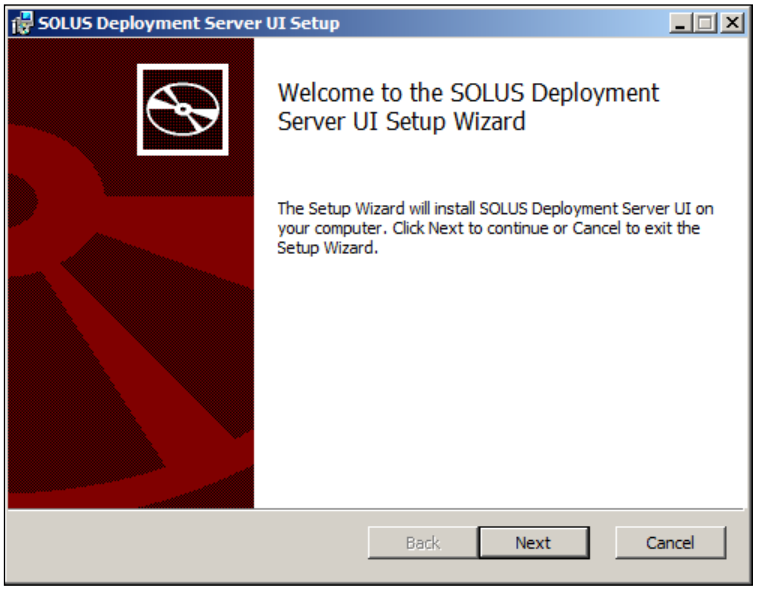
1. From the computer that will host the SOLUS 3 Deployment Service UI, download `SOLUS3DeploymentServerUI.exe` from Capita SIMS to a folder of your choice.
2. Extract the content of the zip file to a folder of your choice. This produces a file named `SOLUS3DeploymentServerDatabase.exe`.
3. Double-click `SOLUS3DeploymentServerUI.exe`.



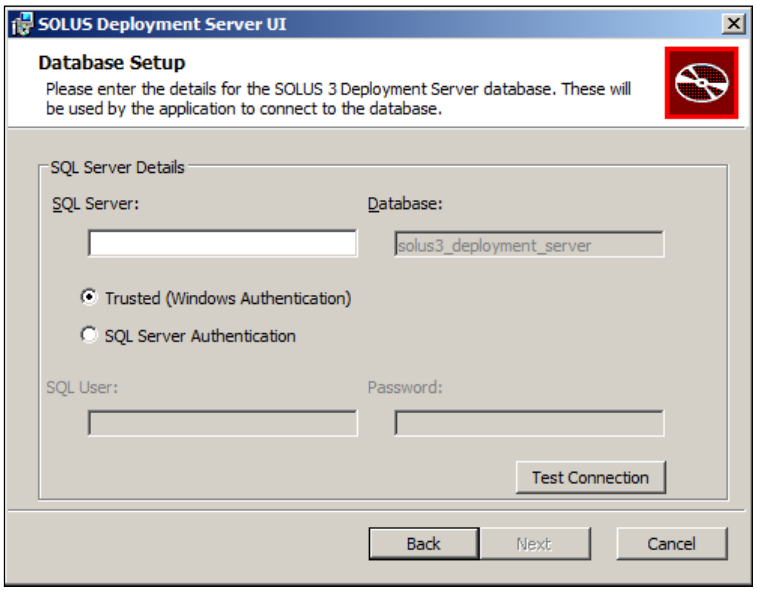
Microsoft .NET Framework 4.5 is selected automatically if it is not yet installed. The appropriate **SOLUS Deployment Server UI** version is selected.

4. Click the **Install** button to display the **SOLUS Deployment Server UI Setup** wizard.

NOTE: Installing Microsoft .NET 4.5 requires a reboot.



5. Click the **Next** button to display the **End-User License Agreement** (EULA).
6. Select the **I accept the terms in the License Agreement** check box.
7. Click the **Next** button to display the **Database Connection Setup** page.



8. In the **SQL Server** field, enter the server\instance for your Deployment Service database, e.g. `MS2012S\SIMS2K14`.

9. Click the **Test Connection** button to validate the connection, and to display the **Database Information** dialog.
   - If the test is successful, click the **OK** button to close the dialog and return to the installer.
   - If the test is unsuccessful, ensure that the server details are correct and that the SQL server is online, and then click the **Test Connection** button again.
10. Click the **Next** button to display the **Set Up Shortcuts** page.
11. Select the check boxes to indicate your shortcut preferences.
12. Click the **Next** button to display the **Destination Folder** page.
13. Use the destination default, or click the **Change** button to select a new installation location.
14. Click the **Next** button to display the **Ready to install SOLUS 3 Deployment Server UI** page.
15. Click the **Install** button to start the file installation, which you can monitor using the progress bar.
16. When the installation process is complete, the Installation successful dialog is displayed.
17. Click the **Finish** button, and then click the **OK** button.

04 | Setting up SOLUS3

Introduction

After installing the SOLUS components, you must register your site with Capita SIMS and configure SOLUS to communicate with the devices in your environment.

Launch SOLUS by selecting **Start | All Programs | SOLUS 3 | SOLUS 3 Deployment Server UI** or via an icon on the desktop.

To enable Local Authorities to install multiple schools for deployment, the facility now exists to utilise the Command Line to enter large amounts of data simultaneously. The Command Line option should be used for the entire set up process, including registration, where its use will eliminate the repetition of entering a large amount of schools individually.

Setting Up SOLUS Checklist

Complete	Description
❑	If the Deployment Service will access the Internet via a proxy, enter the settings in the Deployment Server UI.
❑	Register the Deployment Service.
❑	Designate the Deployment Service Host Computer.
❑	Enter the Update Repository location.
❑	For school sites, define the required workstation settings for the files: ▪ sims.ini ▪ connect.ini ▪ fmsconnect.ini (please see *Workstation Settings* on page *33*).
❑	If you are using email alerts, enter the SMTP Server information.

Complete	Description
❑	If you are using a non-Windows firewall, install agents using Group Policy.
❑	For non-domain networks, install agents, and .NET Framework 4 Full manually on Agent devices.
❑	Define the Deployment Environment and enable SOLUS (please see *Status* on page *30*). More detailed information on defining the Deployment Environment is available later in this handbook (please see *Defining the Deployment Environment* on page *75*).

More Information:
SOLUS3 Configuration on page *30*
Workstation Settings on page *33*
Installing SOLUS3 Agents Manually on page *72*
Installing a SOLUS3 Agent using Group Policy on page *71*

Registering a Site

NOTE: During registration, the Deployment Manager is asked to provide a registration password. The password prevents other establishments from registering as your site inadvertently and is necessary if you need to register again with Capita SIMS. It is important to store this password safely and securely.

The first time that the SOLUS3 UI is run after installation, you will be asked to register the site's Deployment Service with Capita SIMS. The registration process verifies your details and the software you are licensed to use. This process needs to be completed only once. For LAs and regional centres, the registration process also downloads information for any schools under their control (child sites) and their licence information.

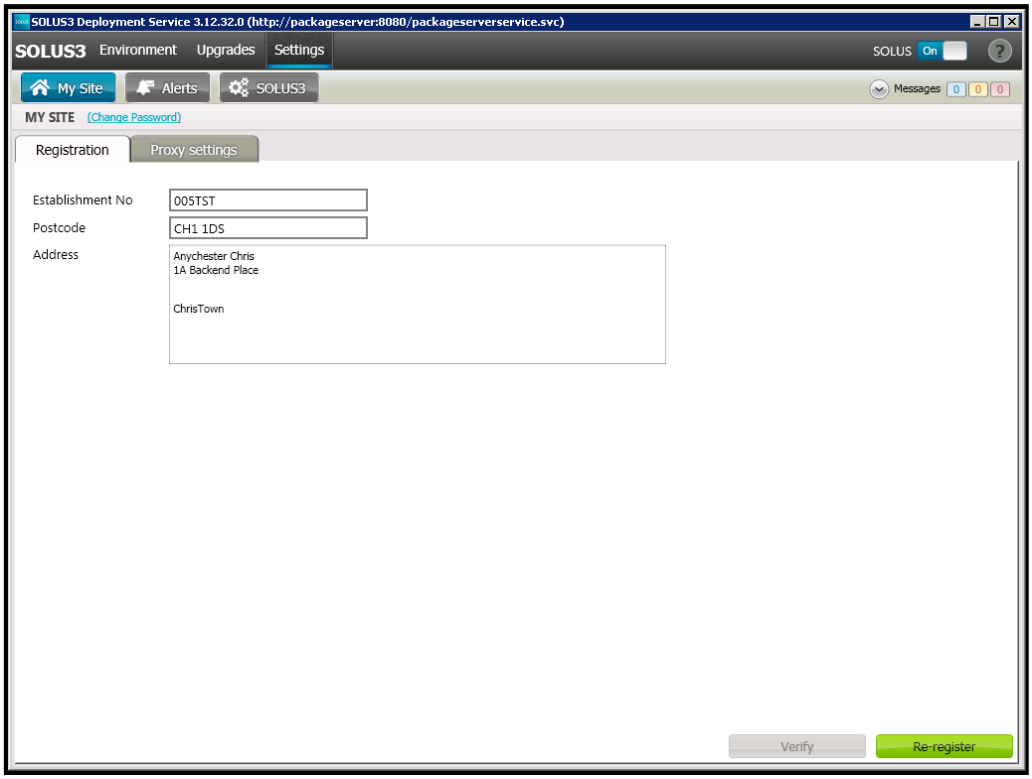
To install multiple sites, the new Command Line feature can be used. This feature enables the user to enter large amounts of data, without having to repeat installation steps (please see *Using the Command Line* on page *125*).

***IMPORTANT NOTE:** If you choose to use the Command Line feature, you must do so from the point of registration.*

To register, you must provide registration details and define the proxy settings (please see *Proxy Settings* on page *29*).

Recording Registration Details

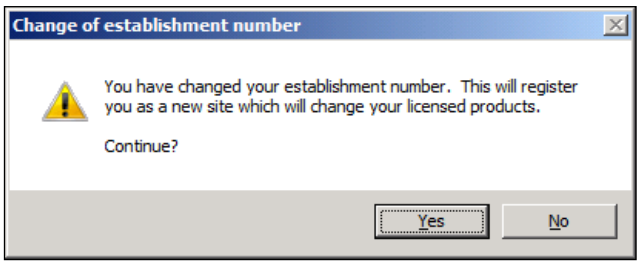
When you open SOLUS following a successful installation, the **MY SITE** page is displayed with the **Registration** tab selected. This tab can be also be displayed by selecting **Environment | My Site** then selecting the **Registration** tab.



*NOTE: If you connect to Capita SIMS servers via an Internet proxy, you must first enter your proxy settings in the **Proxy settings** tab (please see* Proxy Settings *on page* 29*).*

1. To register a site, enter the **Establishment No** and **Postcode** of your school.

   When editing school details via **Environment | My Site**, you must re-register as a different school. This is achieved by clicking the **Re-register** button and confirming that you want to re-register as a different school.



2. Click the **Verify** button to populate the **Address** field.

The address displayed is the address recorded by Capita SIMS for your establishment. Ensure that this information is correct before proceeding to the next step. If your address is not correct, please contact Capita Service Desk.

If the **Verify** button is disabled, you have already registered successfully.

3. Click the **Register** button to display the **User credentials** dialog. This button will be **Re-register** if the site has already been registered successfully.
4. Enter a password in the **Password** and in the **Password confirmation** field.

   Make a note of your password and store it securely. You must have this password if you have to re-register your site (please see *Re-registering your Site with Capita SIMS* on page *28*). Your SOLUS password can be changed by clicking the **Change password** link.
5. Click the **Save** button.
6. Click the **Close** button.

   At this stage, you are redirected to the **SETTINGS** page, where you must enter the mandatory fields. Once this has been completed, you are redirected to the **Targets** page (please see *Setting Targets* on page *50*). However, you can navigate to any other location as required.

More Information:
Proxy Settings on page *29*

Re-registering your Site with Capita SIMS

1. Select **Settings | My Site** to display the **MY SITE** page.
2. Select the **Registration** tab.
3. Click the **Re-register** button to display the **Registration password** dialog.

4. Enter a **Password** and confirm it in the **Password confirmation** field.
5. Click the **Save** button to display the following message:

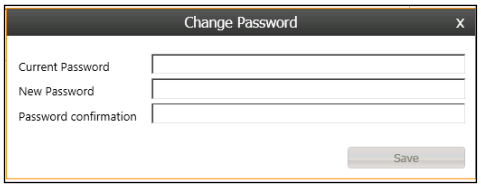
   Contacting CCS update server for registration, this might take a few minutes...
6. Click the **Close** button.

   If you experience any authentication issues, contact the Capita Service Desk.

Changing your Password

To change your password:

1. In the **Current Password** field, enter your existing password.

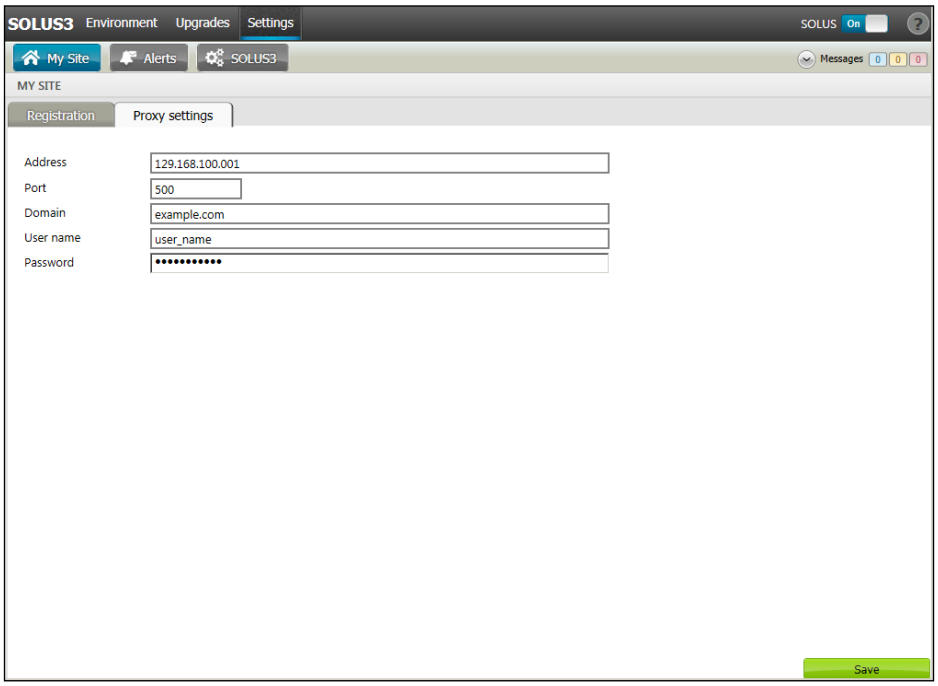


2. Enter your new password in the **Password** and in the **Password confirmation** field.
3. Click the **Save** button to store your changes and to close the dialog.

   If you experience any authentication issues, contact the Capita Service Desk.

Proxy Settings

If your Deployment server connects to Capita SIMS servers via an Internet proxy, you must enter the proxy settings before registering your site.



1. Select **Start | All Programs | SOLUS 3 | SOLUS 3 Deployment Server UI**.
2. Select **Settings | My Site** to display the **MY SITE** page.
3. Select the **Proxy settings** tab to display the proxy setting options.
4. Enter the required proxy settings.

You need only supply the proxy's address and port if:

- your proxy server permits anonymous authentication
- you grant the device hosting the Deployment Service access on the proxy server.

If your proxy server requires a specific account to be used, you must also supply the domain, user name and password.

5. Click the **Save** button.

Option	Description	Example
Address	The IP address for your network's proxy.	129.168.100.001
Port	The port for your network's proxy.	500
Domain	The domain of your network's proxy.	example.com
User name	A user account with access to your network's proxy.	
Password	The password for the user in the **User name** field.	

Status

The top menu bar in SOLUS3 displays the current status of the SOLUS3 DS on the right-hand side.

Initially, SOLUS3 DS is set to **Off**. This enables you to define the DE and configure SOLUS3 without updates being downloaded and deployed unexpectedly.

To switch the SOLUS3 DS on, click the blank space adjacent to the **Off** label. To switch it back off, click the blank space adjacent to the **On** label.

SOLUS3 Configuration

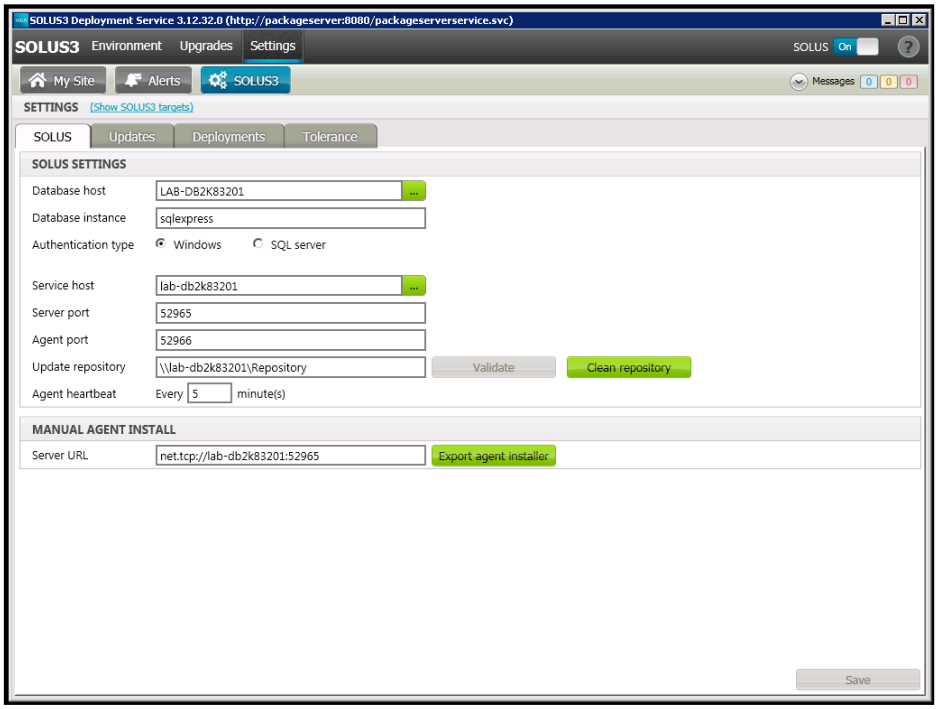
Ensure that your establishment is defined and basic communication settings are configured. After the deployment server has been set up, software can be deployed to the relevant workstations.

Configuring Basic Settings in SOLUS

The **SOLUS** tab provides access to settings for the SOLUS database and the communication ports (please see *Configuring the SOLUS Database and Configuration Ports* on page *31*). It also has an option to produce files for manual agent installation (please see *Creating Installation Files for a Manual Agent Installation* on page *33*).

Configuring the SOLUS Database and Configuration Ports

This panel contains settings for the SOLUS database and the communication ports and were entered during the installation process. These settings should only be changed if absolutely necessary, for instance if there is a port conflict. Always consult your local support unit in these cases, and contact the Capita Service Desk if you have any queries.



1. Select **Settings | SOLUS3** to display the **SETTINGS** page.
2. Select the **SOLUS** tab to display the **SOLUS SETTINGS** panel and verify the panel contents.

> *NOTE: Use caution when completing this page.*

3. In the **Database host** field, click the green **Browse** button to locate the correct host.
4. In the **COMPUTER SELECTION** panel, select **Active Directory** or **Network** depending on your network setup and location of your host, select **Agents** to browse computers with SOLUS3 agents only.

   Active Directory

   Select the required OU or change domain.

   a. To change domain, click the **Change Domain** button.

   b. From the drop-down menu, select the domain.

   c. Enter your **Login name** and **Password**, and then click the **Save** button.

   This option also enables you to use Organisational Units (OUs).

Network

a. From the **AVAILABLE COMPUTERS** column, double-click the required computer to select it. Alternatively, use the **Move (>)** button.

b. Click the **OK** button.

Agents

a. From the **AVAILABLE COMPUTERS** column, double-click the required computer to select it. Alternatively, use the **Move (>)** button.

b. Click the **OK** button.

5. In the **Database instance** field, enter the instance name of the deployment database.
6. Select the required **Authentication type** radio button:
   - Select **Windows** to use your Windows login credentials; or
   - Select **SQL server** then enter your SQL **Username**, **Password** and **Confirm Password**.
7. In the **Service host** field, click the green **Browse** button then locate the computer that hosts the DS (please see step 4).
8. In the **Server port** field, enter the port that the DS uses to connect to agents.
9. In the **Agent port** field, enter the port that the agents use to connect to the DS.

   NOTE: Exercise caution when you enter the Agent port number. After the DS has been defined and the agents have been deployed, any changes made to this number have to be made manually on each agent instance. Therefore, verify that the Agent port number will not have to be changed under normal circumstances.

10. In the **Update repository** field, set the computer and directory that stores the updates for the DE, using the following syntax:

    `\\<computername>\<repository>`

    The Windows user `System` must have read/write access to the Update Repository directory. The default update interval is 40 minutes.

    NOTE: This folder must exist and must be presently accessible.

11. In the **Validate** field, click the **Validate** button to verify that the address entered for the **Update Repository** is a valid network share.
12. Click the **Clean repository** button to delete packages that are over a year old (excluding infrastructure packages). This maximises space available in the repository.
13. In the **Agent heartbeat** field, enter a time in the minute(s) field to define how often the agent sends the message. This defaults to five minutes.
14. Click the **Save** button. SOLUS deploys its agents to the relevant computers automatically.

> *NOTE: To ensure optimal performance, the system clock on all devices in the SOLUS3 DE (including all devices with an agent) must be set to a common network time server.*

Creating Installation Files for a Manual Agent Installation

This panel enables you to produce files for manual agent installation. This is used in cases where automatic Agent installation has not been successful.

1. Select **Settings | SOLUS3** to display the **SETTINGS** page.
2. Select the **SOLUS** tab.
3. In the **MANUAL AGENT INSTALL** panel, the content of the **Server URL** field is calculated from the service host field and the server port. As a result, the field is read-only.

   If you need to install a SOLUS3 agent manually, you will be prompted to enter this Server URL.
4. Click the **Export agent installer** button to export the installer files.
5. Navigate to the storage location. Use an easily accessible location, such as a network drive or removable media.
6. Click the **OK** button. A message is displayed briefly to indicate that the export has been successful.
7. Verify that the following files have been created:
   - `AgentInstaller.js`
   - `Solus3.Keys.DeploymentService.Public.xml`
   - `SOLUS3AgentInstaller.bat`
   - `SOLUS3AgentInstaller_x86.msi`
   - `SOLUS3AgentInstaller_x64.msi`

   A batch file that can be edited to suit your installation needs is provided. For more information, please refer to the *Using batch files* Microsoft TechNet article (http://technet.microsoft.com/en-us/library/bb490869.aspx).

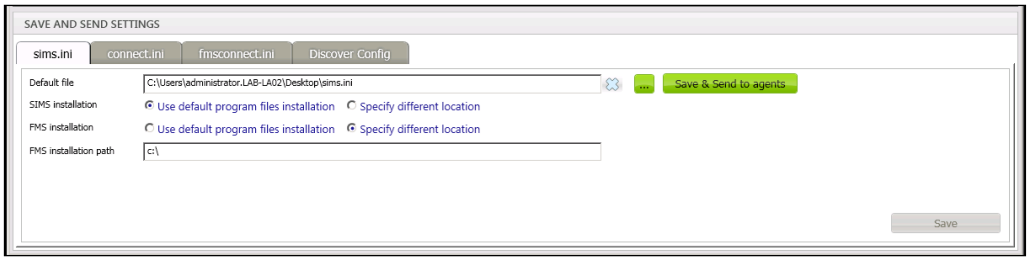
Workstation Settings

If you are registering as a school site, in addition to defining your Deployment Server and Update Repository, you must also enter workstation settings before defining the rest of your environment and deploying updates.

After you have selected the required site, site-specific settings can be configured for:

- the SIMS.ini file (please see *Configuring Site-Specific SIMS.ini Settings* on page *34*).
- the Connect.ini file (please see *Configuring Site-Specific Connect.ini Settings* on page *35*).
- the FMSconnect.ini file (please see *Configuring Site-Specific FMSconnect.ini Settings* on page *36*).

- the Discover file (please see *Configuring Discover-Specific Settings* on page *37*).



IMPORTANT NOTE: *If you have not purchased SIMS, FMS or Discover, the named tab is not displayed.*

Configuring Site-Specific SIMS.ini Settings

Use this function to configure site-specific information for the `sims.ini` file. Clicking the **Save & Send to agents** button sends a `sims.ini` file to each device.

IMPORTANT NOTE: *Any device-specific `sims.ini` values, such as the `SIMSInfrastructureSetup` value, will be safeguarded.*

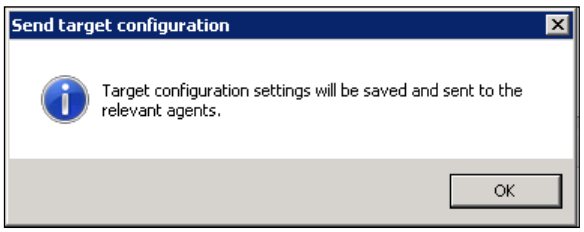
1. Select **Environment | Configure Workstations** to display the **SCHOOL SELECTION** page.
2. Select the required site.

   This step applies only if you are an LA or if you have multiple sites to select from. If this step does not apply to you, proceed to the next step.
3. In the **SAVE AND SEND SETTINGS** panel, select the **sims.ini** tab to display the customisation options.

4. Click the green **Browse** button adjacent to the **Default file** field to display the **Open** dialog.
5. Locate and select the required `sims.ini` file for the site's SIMS workstations. Click the blue cross to clear your entry, if it was entered in error.

> ***IMPORTANT NOTE:*** *The default `sims.ini` file must not have a `SIMSDotNetDirectory` value defined. SOLUS3 takes this value from the* ***SIMS.net installation*** *field and adds it to the `sims.ini` file that is sent to the SIMS workstations.*

6. For the SIMS/FMS installation path, select the appropriate radio buttons:
   - **Use default program files installation**
   - **Specify different location. Enter the alternative installation location**.
7. Click the **Save** button to store the settings only.
8. Click the **OK** button to confirm the **Save target configuration** dialog.
9. Click the **Save & Send to agents** button to display the **Send target configuration** dialog.



10. Click the **OK** button to confirm the deployment.

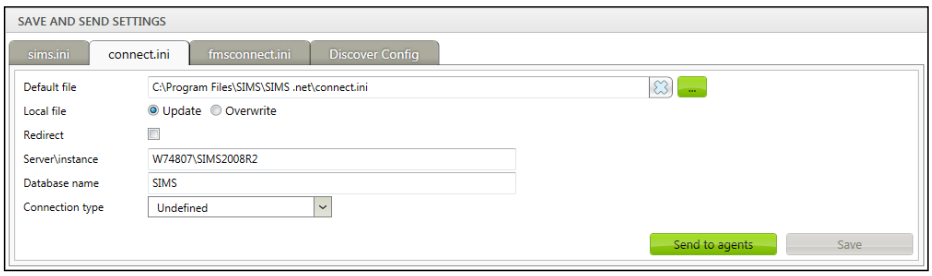
Configuring Site-Specific Connect.ini Settings

Use this function to configure site-specific information for the `connect.ini` file. When you click the **Send connect.ini to agents** button, SOLUS3 sends the new `connect.ini` file to each device.

> ***IMPORTANT NOTE:*** *Any values not defined in SOLUS3, or in the default `connect.ini` file, will remain unchanged unless you select the option to overwrite all values in the local `connect.ini` file.*

1. Select **Environment | Configure Workstations** to display the **SCHOOL SELECTION** page.
2. Select the required site.

   This step applies only if you are an LA or if you have multiple sites to select from. If this step does not apply to you, go to the next step.
3. In the **SAVE AND SEND SETTINGS** panel, select the **connect.ini** tab to display the customisation options.



4. Click the green **Browse** button adjacent to the **Default file** field to display the **Open** dialog.
5. Locate and select the required `connect.ini` file.
6. Click the **Open** button to return to the **Workstation settings** panel.

   If entered in error, click the blue cross to clear your entry.

   If the **Server\instance name**, **Database name**, and **Connection type** values are defined in the `connect.ini` file, the appropriate fields are populated automatically.

   If the default `connect.ini` file contains a redirect location, SOLUS selects the **Redirect** check box and populates the **Redirect file location** field.
7. To add any missing values to the `connect.ini` file, select the **Update** radio button. To replace all values in the `connect.ini` file, select the **Overwrite** check box.
8. Select a **Connection type**.
9. Click the **Save** button to store the settings.
10. Click the **OK** button to confirm the **Save target configuration** dialog.
11. Click the **Send to agents** button to display the **Send target configuration** dialog.
12. Click the **OK** button to confirm the deployment.

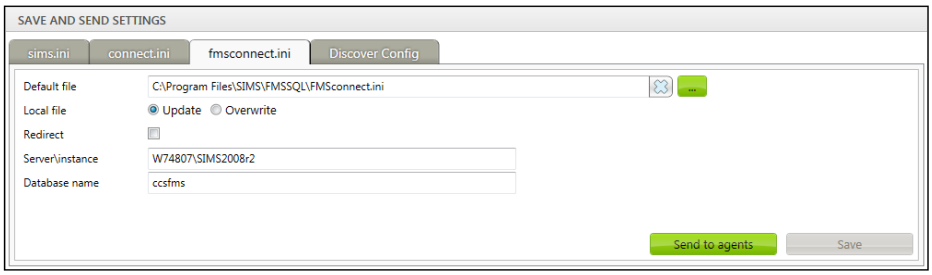
Configuring Site-Specific FMSconnect.ini Settings

If you have purchased FMS, use this function to configure site-specific information for the `fmsconnect.ini` file. When you click the **Send fmsconnect.ini to agents** button, SOLUS3 sends the new `fmsconnect.ini` file to each device.

> ***IMPORTANT NOTE:*** *Any values not defined in SOLUS3 or the default `fmsconnect.ini` file will remain unchanged unless you have selected the option to overwrite all values in the local `fmsconnect.ini` file (please see step 7).*

1. Select **Environment | Configure Workstations** to display the **SCHOOL SELECTION** page.
2. Select the required site.

   This step applies only if you are an LA or if you have multiple sites to select from. If this step does not apply to you, go to the next step.
3. In the **SAVE AND SEND SETTINGS** panel, select the **fmsconnect.ini** tab to display the customisation options.



4. Click the **Browse** button adjacent to the **Default file** field to display the **Open** dialog.
5. Locate and select the required `fmsconnect.ini` file.
6. Click the **Open** button to return to the **Configure Workstation** panel.

   If entered in error, click the blue cross to clear your entry.

   If the **Server\instance name** and the **Database name** values are defined in the `fmsconnect.ini` file, the appropriate fields are populated automatically.

   If the default `fmsconnect.ini` file contains a redirect location, SOLUS automatically selects the **Redirect** check box and populates the **Redirect file location** field.
7. To add any missing values to the `fmsconnect.ini` file, select the **Update** radio button. To replace all values in the `fmsconnect.ini` file, select the **Overwrite** check box.
8. Select the **Redirect** check box if you wish to redirect to a different `fmsconnect.ini` file. Selecting this check box enables you to record the **Redirect file** location.
9. Click the **Save** button.
10. Click the **OK** button to confirm the **Save target configuration** dialog.
11. Click the **Send to agents** button to display the **Send target configuration** dialog.
12. Click the **OK** button to confirm the deployment.

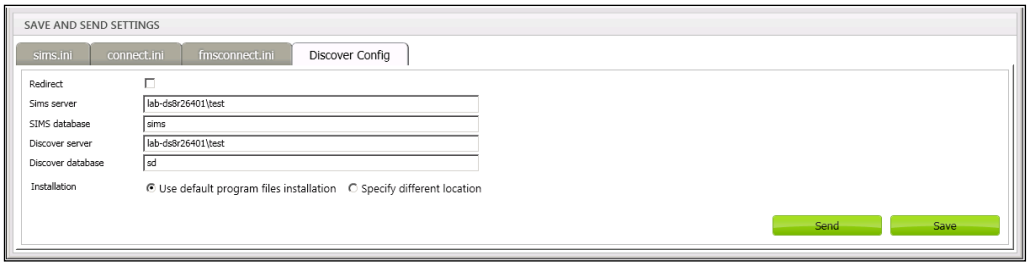
Configuring Discover-Specific Settings

Select the **Discover Config** tab to view and configure site-specific information for the Discover clients. You can use the redirect functionality to update the Discover client configuration file.

1. Select **Environment | Configure Workstations** to display the **SCHOOL SELECTION** page.
2. Select the required site.

   This step applies only if you are an LA or if you have multiple sites to select from. If this step does not apply to you, go to the next step.
3. In the **SAVE AND SEND SETTINGS** panel, select the **Discover Config** tab to display the current settings.

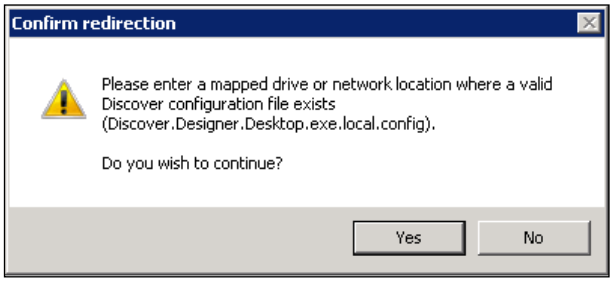
   The server and database fields are populated automatically with the current **Discover Database** target definitions and cannot be changed manually in the **Discover Config** tab.



NOTE: This option is available only if Discover client(s) have been setup.

If Discover clients uses a centrally hosted configuration file and redirection is required, proceed as follows:

4. To redirect the Discover clients, select the **Redirect** check box to display a confirmation dialog.



5. Click the **Yes** button to confirm that you want to proceed.
6. To set the **Redirect file location**, enter the location path of the configuration file in the **Redirect file location** field. Alternatively, click the green **Browse** button adjacent to the field, navigate to the location of the required `Discover.Designer.Desktop.exe.config` file, and then double-click the appropriate folder.
7. For the application installation path, select one of the following:
   - Use default program files installation
   - Specify different location.

     Enter the alternative installation location.
8. Click the **Save** button to store the settings only.
9. Click the **OK** button to confirm the **Save** dialog.
10. Click the **Send** button to display the **Discover configuration** dialog.
11. Click the **OK** button to confirm the deployment.

***IMPORTANT NOTE**: When the Discover clients have been redirected using this procedure, you can revert to the original settings by changing the Discover configuration file manually.*

Working with Backups

***IMPORTANT NOTE**: Although SOLUS makes backups of the databases to which it deploys updates, this is not a substitute for a regular and comprehensive database backup plan.*

When SOLUS3 deploys an update, the default behaviour is to create backups of all affected databases.

If you select the **Delete database backups at the end of this deployment** check box at the bottom of the **Update deployment** or **Deployment history** pages, the default action for a deployment will be to delete the database backups made by SOLUS3. This can be changed on a per-deployment basis when scheduling the deployment.

05 | Entering SOLUS3 System Settings

Introduction

After registering a site with Capita SIMS, the Deployment Manager must provide the SOLUS3 DS parameters.

> *NOTE: The correct settings must be entered and saved before SOLUS3 can begin to deploy agents and updates.*

Status

The top menu bar in SOLUS3 displays the current status of the SOLUS3 DS on the right-hand side.

Initially, SOLUS3 DS is set to **Off**. This enables you to define the DE and configure SOLUS3 without updates being downloaded and deployed unexpectedly.

To switch the SOLUS3 DS on, click the blank space adjacent to the **Off** label. To switch it back off, click the blank space adjacent to the **On** label.

SOLUS3 Configuration

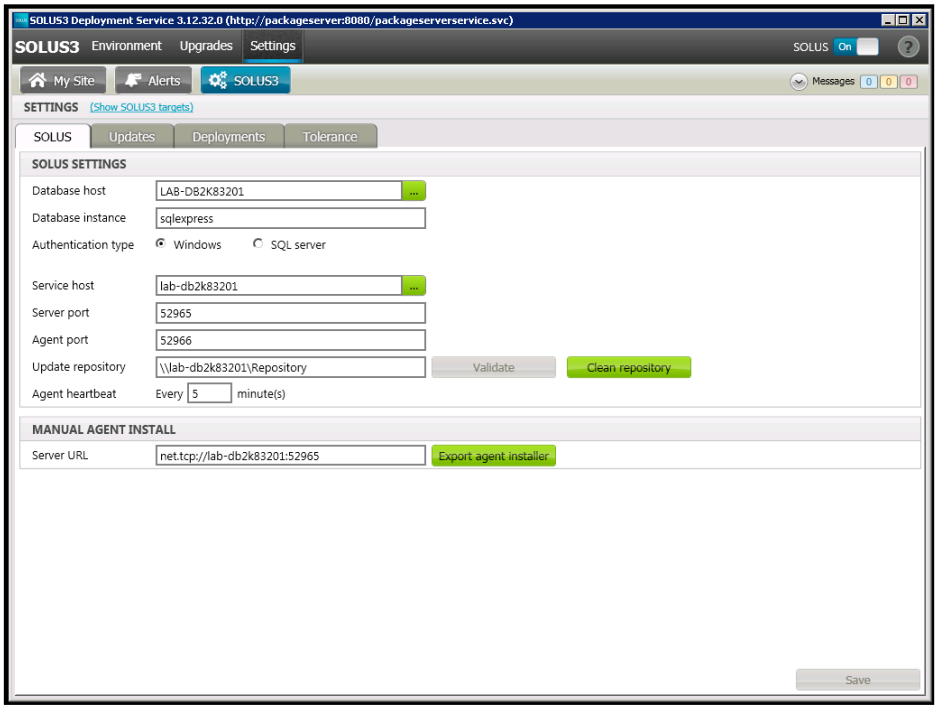
Ensure that your establishment is defined and basic communication settings are configured. After the deployment server has been set up, software can be deployed to the relevant workstations.

Configuring Basic Settings in SOLUS

The **SOLUS** tab provides access to settings for the SOLUS database and the communication ports (please see *Configuring the SOLUS Database and Configuration Ports* on page *31*). It also has an option to produce files for manual agent installation (please see *Creating Installation Files for a Manual Agent Installation* on page *33*).

Configuring the SOLUS Database and Configuration Ports

This panel contains settings for the SOLUS database and the communication ports and were entered during the installation process. These settings should only be changed if absolutely necessary, for instance if there is a port conflict. Always consult your local support unit in these cases, and contact the Capita Service Desk if you have any queries.



1. Select **Settings | SOLUS3** to display the **SETTINGS** page.
2. Select the **SOLUS** tab to display the **SOLUS SETTINGS** panel and verify the panel contents.

> *NOTE: Use caution when completing this page.*

3. In the **Database host** field, click the green **Browse** button to locate the correct host.
4. In the **COMPUTER SELECTION** panel, select **Active Directory** or **Network** depending on your network setup and location of your host, select **Agents** to browse computers with SOLUS3 agents only.

   Active Directory

   Select the required OU or change domain.

   a. To change domain, click the **Change Domain** button.

   b. From the drop-down menu, select the domain.

   c. Enter your **Login name** and **Password**, and then click the **Save** button.

      This option also enables you to use Organisational Units (OUs).

Network

a. From the **AVAILABLE COMPUTERS** column, double-click the required computer to select it. Alternatively, use the **Move (>)** button.

b. Click the **OK** button.

Agents

a. From the **AVAILABLE COMPUTERS** column, double-click the required computer to select it. Alternatively, use the **Move (>)** button.

b. Click the **OK** button.

5. In the **Database instance** field, enter the instance name of the deployment database.
6. Select the required **Authentication type** radio button:
   - Select **Windows** to use your Windows login credentials; or
   - Select **SQL server** then enter your SQL **Username**, **Password** and **Confirm Password**.
7. In the **Service host** field, click the green **Browse** button then locate the computer that hosts the DS (please see step 4).
8. In the **Server port** field, enter the port that the DS uses to connect to agents.
9. In the **Agent port** field, enter the port that the agents use to connect to the DS.

   NOTE: Exercise caution when you enter the Agent port number. After the DS has been defined and the agents have been deployed, any changes made to this number have to be made manually on each agent instance. Therefore, verify that the Agent port number will not have to be changed under normal circumstances.

10. In the **Update repository** field, set the computer and directory that stores the updates for the DE, using the following syntax:

    `\\<computername>\<repository>`

    The Windows user `System` must have read/write access to the Update Repository directory. The default update interval is 40 minutes.

    NOTE: This folder must exist and must be presently accessible.

11. In the **Validate** field, click the **Validate** button to verify that the address entered for the **Update Repository** is a valid network share.
12. Click the **Clean repository** button to delete packages that are over a year old (excluding infrastructure packages). This maximises space available in the repository.
13. In the **Agent heartbeat** field, enter a time in the minute(s) field to define how often the agent sends the message. This defaults to five minutes.
14. Click the **Save** button. SOLUS deploys its agents to the relevant computers automatically.

> *NOTE: To ensure optimal performance, the system clock on all devices in the SOLUS3 DE (including all devices with an agent) must be set to a common network time server.*

Creating Installation Files for a Manual Agent Installation

This panel enables you to produce files for manual agent installation. This is used in cases where automatic Agent installation has not been successful.

1. Select **Settings | SOLUS3** to display the **SETTINGS** page.
2. Select the **SOLUS** tab.
3. In the **MANUAL AGENT INSTALL** panel, the content of the **Server URL** field is calculated from the service host field and the server port. As a result, the field is read-only.

   If you need to install a SOLUS3 agent manually, you will be prompted to enter this Server URL.
4. Click the **Export agent installer** button to export the installer files.
5. Navigate to the storage location. Use an easily accessible location, such as a network drive or removable media.
6. Click the **OK** button. A message is displayed briefly to indicate that the export has been successful.
7. Verify that the following files have been created:
   - `AgentInstaller.js`
   - `Solus3.Keys.DeploymentService.Public.xml`
   - `SOLUS3AgentInstaller.bat`
   - `SOLUS3AgentInstaller_x86.msi`
   - `SOLUS3AgentInstaller_x64.msi`

   A batch file that can be edited to suit your installation needs is provided. For more information, please refer to the *Using batch files* Microsoft TechNet article (http://technet.microsoft.com/en-us/library/bb490869.aspx).

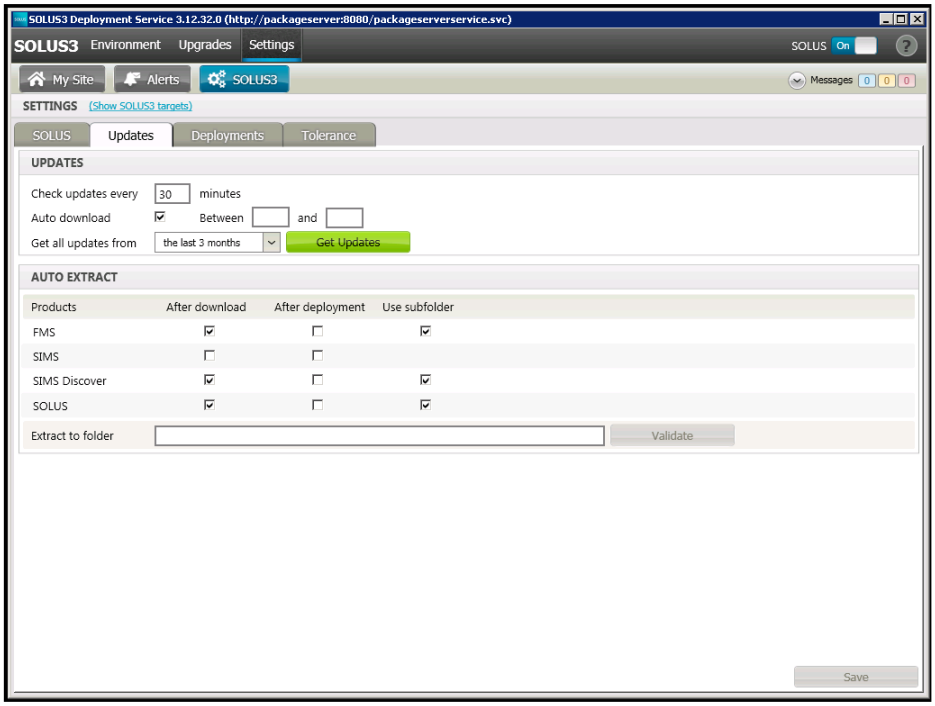
Configuring Updates and Agents

This tab provides access to all functions that relate to software updates, agents and software deployments.

> *NOTE: Auto deployments apply to schools only.*

Configuring Software Update Downloads

The **Updates** panel enables the administrator to set options relating to the download of updates.



1. Select **Settings | SOLUS3** to display the **SETTINGS** page.
2. Select the **Updates** tab.
3. In the **UPDATES** panel , enter the number of minutes between DS checks for authorised updates in the **Check updates every** field. This defaults to 30 minutes. Valid times are from 30 to 120 minutes.
4. If you select the **Auto download** check box, you will also need to specify when the deployment server will download newly available updates automatically to the update repository.

   The **AUTO EXTRACT** panel enables you to decide whether the product is extracted automatically **After download** or **After deployment** for each available product by selecting the relevant check boxes.

   If you use an alternative method to update SIMS, you can choose to extract the SIMS package automatically. A set of files (including `SIMSApplicationSetup.exe`, `SIMSSQLApplicationSetup.exe`, etc.) is posted in the specified folder, ready for manual installation via a setups directory.

   This panel also enables you to identify the location of the extracted files.
5. Enter the folder name to which you wish to extract the update files in the **Extract to folder** field.

> ***IMPORTANT NOTES:*** *The folder name must be a UNC path. It is not possible to record a path to a mapped network folders.*
>
> *Careful consideration should be given when specifying the location to which the files are extracted. The specified path must be a secure location, accessible only by authorised personnel.*
>
> *If you are using a live setups folder, the* ***Extract to folder*** *should relate to the* `Setups` *folder and only the FMS* ***Use subfolder*** *check box should be selected.*

6. For each product that you wish to extract automatically, select the **Auto extract** check box. This will extract the product to the **Extract to folder** specified in Step 5.

   For each product selected for automatic extraction, you can choose to extract them to separate sub-folders. The sub-folder is named according to the product, e.g. SIMS, FMS, etc.

7. Select the **Use subfolder** check box to extract the selected product to a sub-folder. In the previous example, the path to the sub-folder for the SIMS product would be `\\W8144\Extraction\SIMS`.

8. Click the **Validate** button to check that the specified folder exists and that you have the appropriate permissions.

Configuring Automatic Deployments

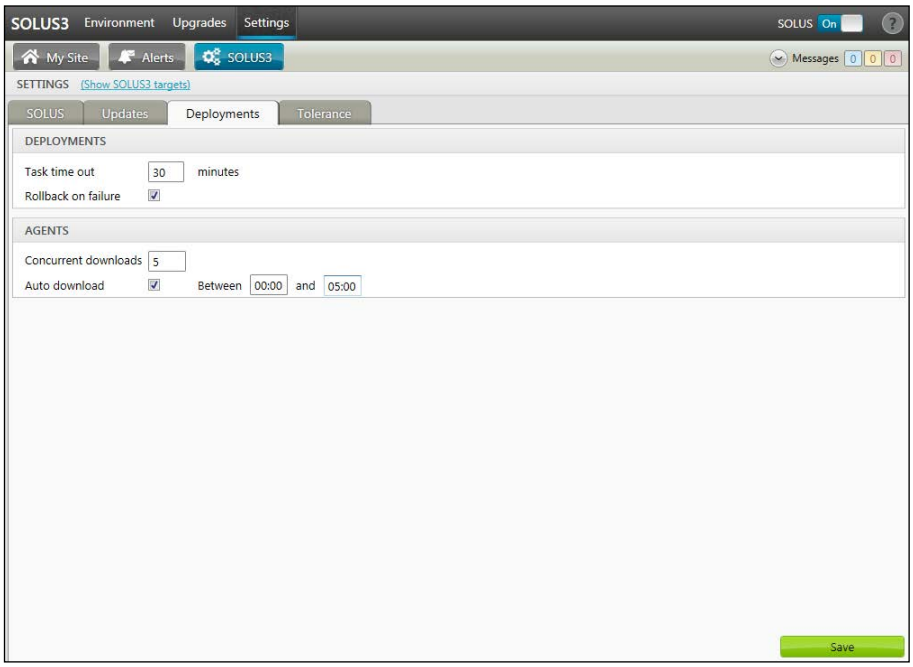
Automatic deployments are part of the basic settings of the DS, and enable administrators of school sites to schedule the automatic deployment of updates to devices. These updates can relate to products and services.

> ***IMPORTANT NOTE:*** *By default, all installations are set to deploy automatically. The default time will be set to daily between 03:30 and 05:30.*

Automatic deployment scheduling is based on product groups; if a group is included in the schedule, then all authorised updates within that group will be deployed at the scheduled time. For example, if there is an authorised update for the SIMS workstation target type and an authorised update for the SIMS DMS target type, both updates will be deployed the next time that the SIMS group auto deployment is scheduled to run. For more granular control over which particular updates are deployed, you can remove authorisation from updates you temporarily wish to skip.

1. Select **Settings | SOLUS3** to display the **SETTINGS** page.

2. Select the **Deployments** tab to display the **DEPLOYMENTS** panel.



3. In the **Task time out** field of the **DEPLOYMENTS** panel, enter the number of minutes the DS must wait for a response from an agent before considering the deployment for that agent a failure. This defaults to 30 minutes. Valid times are between 30 and 120 minutes.
4. If you select the **Rollback on failure** check box, SOLUS3 will attempt to roll back all devices to their previous state when the task failure tolerance has been exceeded.
5. Click the **Save** button to store your settings.
6. In the **AUTO DEPLOYMENTS** panel, select the check box of one or more products you want to **Auto deploy**. Selecting a check box displays additional options.

   Enter the times between which you want the automatic deployments to start in 24-hour format. The minimum time span is 120 minutes.
7. For each product, select the check box relating to the required days.
8. Click the **Save** button to store your settings.

> ***IMPORTANT NOTES****: Not all updates can be deployed automatically. Updates that can be deployed automatically are identifiable by the letter* ***A*** *in the penultimate column in* ***Upgrades | Update Library | Updates****.*

Configuring Agents

Configure the basic agent settings in the **AGENTS** panel. This enables the administrator to set options relating to the download of updates.

1. Select **Settings | SOLUS3** to display the **SETTINGS** page.

2. Select the **Deployments** tab to display the **AGENTS** panel.

3. In the **Concurrent downloads** field, set the maximum number of agents that can download from the Update Repository at a time.
4. If you select the **Auto download** check box, the DS sends the updates to the appropriate agents automatically. However, this sends updates to devices only if the updates are not installed. Enabling this option can prevent network congestion that might otherwise occur if updates were delivered to all agents at once.
5. In the **Between** <time> **and** <time> fields, enter a valid time span for the automatic downloads in 24-hour format.
6. Click the **Save** button to store your settings.

IMPORTANT NOTE: *The Windows user named System must have read/write access to the Update Repository directory.*

Selecting the ***Auto download*** *option does not install the update. Downloading updates to an agent places the required update file on the target; the updates must still be deployed.*

TIP: Due to the large file sizes involved in some updates, Capita SIMS recommends that you set the automatic download options to times when bandwidth requirements for other users are at a minimum.

For SOLUS3 to download updates to a device automatically, the device must be turned on. Therefore, it may be necessary to set the ***Concurrent downloads*** *value to a low number and set the process to run during working hours.*

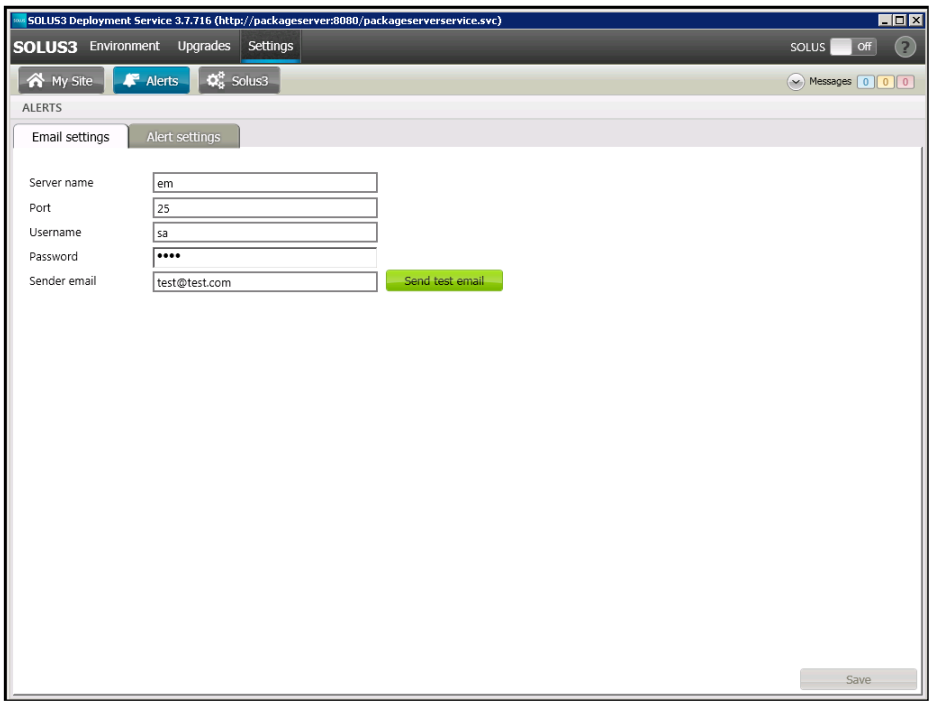
When you plan to distribute large updates to a large number of agents, begin the download of updates in advance of the deployment date. SOLUS3 can span downloads over several days. For example, if the download time is set between 08:00 and 10:00, SOLUS3 will download an update file to as many agents as possible during that two-hour period each day, until each agent has received the update files.

Configuring Alerts

The **Alerts** page enables you to configure SOLUS3 email settings (please see *Managing Email Settings* on page *49*) and alert settings (please see *Managing Alert Settings* on page *50*).

Managing Email Settings

The **ALERTS** page enables Deployment Managers to set up SOLUS3 to send emails when certain SOLUS3 events occur. Such events are configurable in the **Alert Settings** tab.

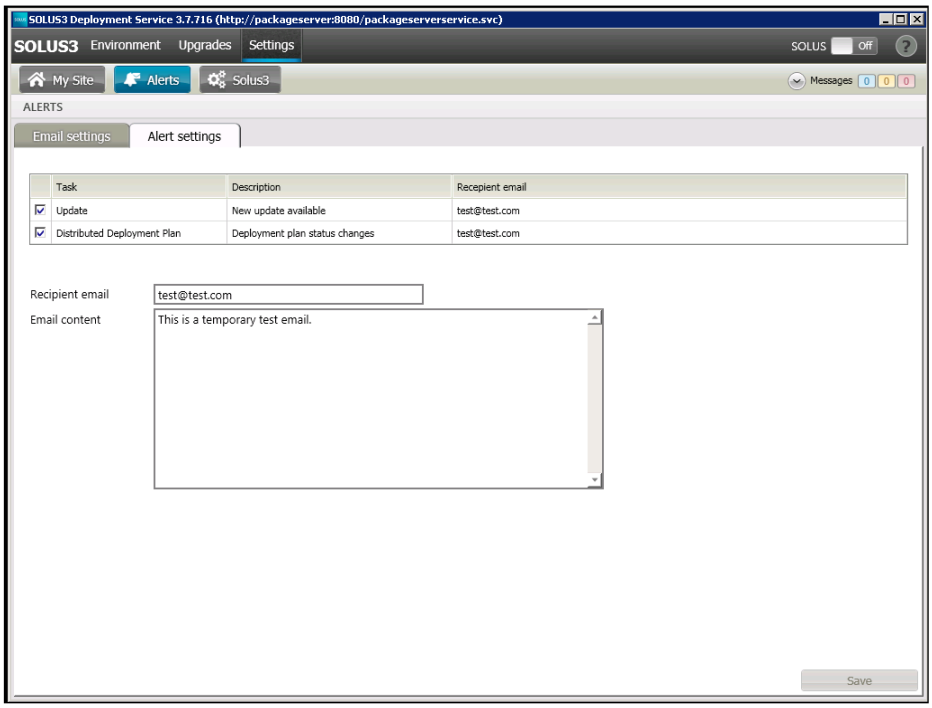


1. Select **Settings | Alerts** to display the **ALERTS** page.
2. Select the **Email settings** tab.
3. In the **Server name** field, enter the name of the SMTP server that will send out alert emails.
4. In the **Port** field, enter port number of the SMTP server that will send out alert emails. The port number defaults to **25**.
5. In the **User name** field, enter the user name for the account that will be sending the alert notifications.
6. In the **Password** field, enter password for the account that will be sending the alert notifications.
7. In the **Sender email** field, enter the full email address for the account that will send alert notifications.
8. Click the **Send test email** button to test your configuration. Failure generates the error message **Failed to send test email to test@test.com**. Success does not generate a message.
9. Click the **Save** button to store your changes.

Managing Alert Settings

After entering the server and user details in the **Email Settings** tab, select which events should trigger an alert email. The subject line for each alert email will contain important information, such as the event type and the time of the event. Additional information, such as contact names and addresses, can be added to the email body. An Update task will trigger an email after an update has been authorised to the school and a Distributed Deployment Plan will trigger an email when a deployment has completed.

1. Select **Settings | Alerts** to display the **ALERTS** page.
2. Select the **Alert settings** tab to display a list of available alerts.

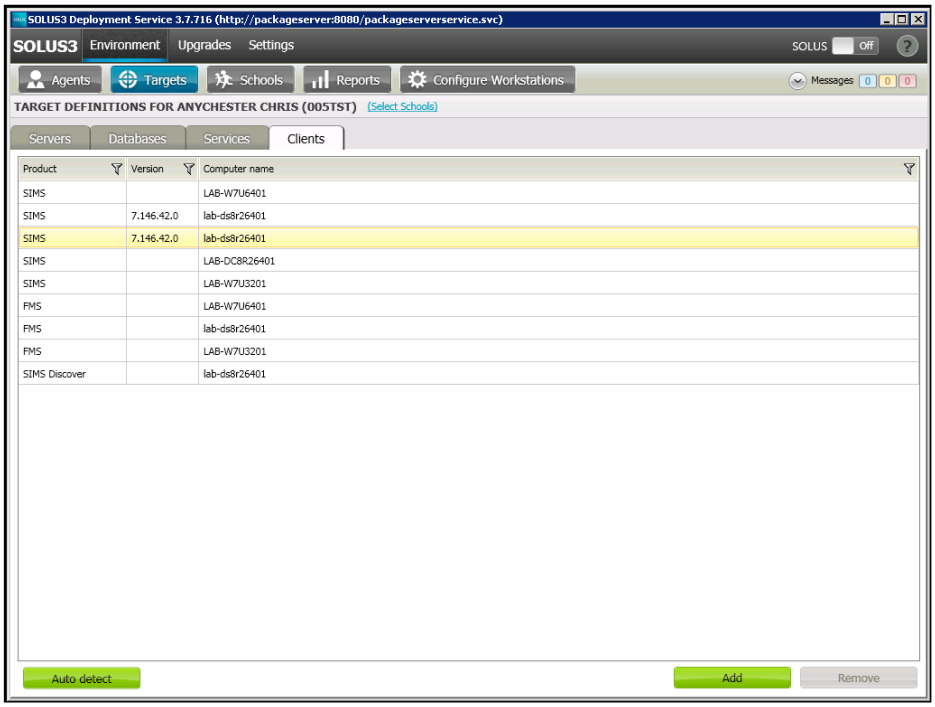


3. To activate an alert, select its check box. To de-activate an alert, deselect it.
4. To edit the **Recipient email** or the email content, highlight the required task in the table.
5. Edit the **Recipient email** address.
6. Edit the email content.
7. Click the **Save** button. The message **Distributed Deployment Plan alert successfully saved** is displayed briefly.

Setting Targets

The **Targets** page enables you to set up your servers (please see *Servers* on page *51*), databases (please see *Databases (SIMS, FMS)* on page *53*), services (please see *Selecting Services* on page *55*) and clients (please see *Adding Clients* on page *63*).

All of these work together to deliver and install the necessary services and products to your workstations.



To set targets:

1. Select **Environment | Targets** to display the **TARGET DEFINITIONS** page.
2. Optionally select one or more required schools.

   This generally applies to Local Authorities only.

   a. Click the **Select Schools** link.

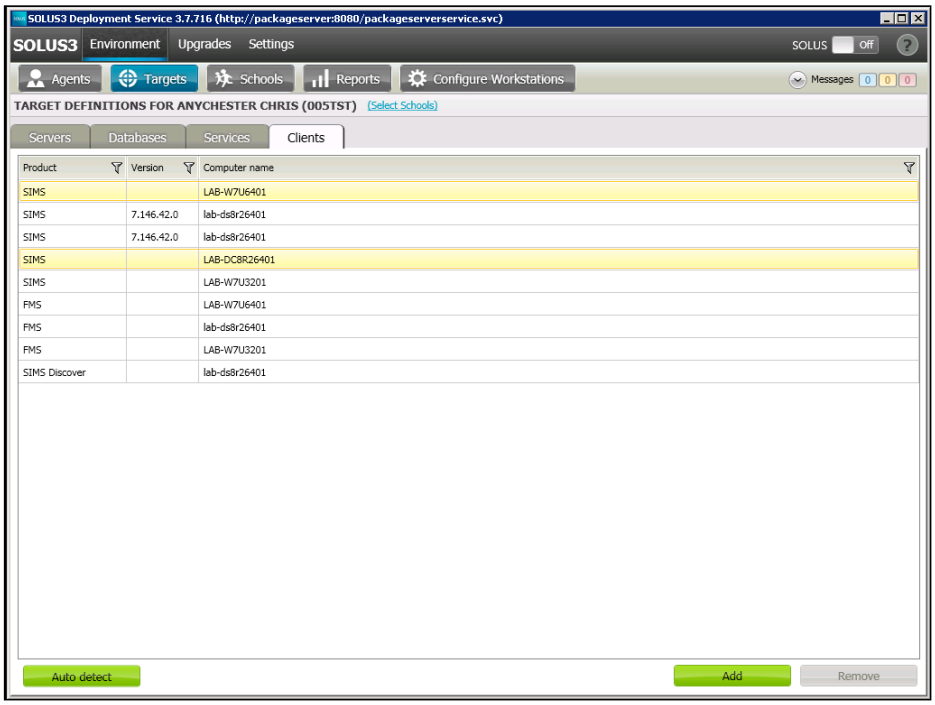
   b. Select the required school(s).

   c. Click the **OK** button.

Servers

1. Select **Environment | Targets** to display the **TARGET DEFINITIONS** page.

2. Select the **Servers** tab.



Adding a Server

1. Click the **Add** button to add the **DEFINE A NEW SQL SERVER TARGET** panel to the **TARGET DEFINITIONS** page.
2. Select **FMS** or **SIMS** as required.
3. To record the **Server name**, click the **Select** button and select one of the following radio buttons:
   - **Active Directory**, and then select **Domain Controllers** or **MOSS** (Microsoft Office SharePoint Server), and then click the **Select** button.
   - **Network**
   - **Agents**.
4. Select the computer name in the **AVAILABLE COMPUTERS** panel, and then click the Right-Arrow button (). This moves the selected computer(s) from the **AVAILABLE COMPUTERS** panel to the **SELECTED COMPUTERS** panel. Alternatively, search and add computers from the **SELECTED COMPUTERS** panel.
   a. Enter the **Computer Name** or the **IP Address** you are looking for.
   b. To search and add, click the **Add** button ().

      This button is available only if you enter a name that (partially) meets an available computer name. Wildcards cannot be used.

      Adding computers in this way displays them in the **SELECTED COMPUTERS** panel with their FQDN (Fully Qualified Domain Name).
5. Click the **OK** button to add the server name.
6. Enter the **Instance name**.
7. Enter the **Binn folder** location.

8. Click the **Save** button.

Editing a Server

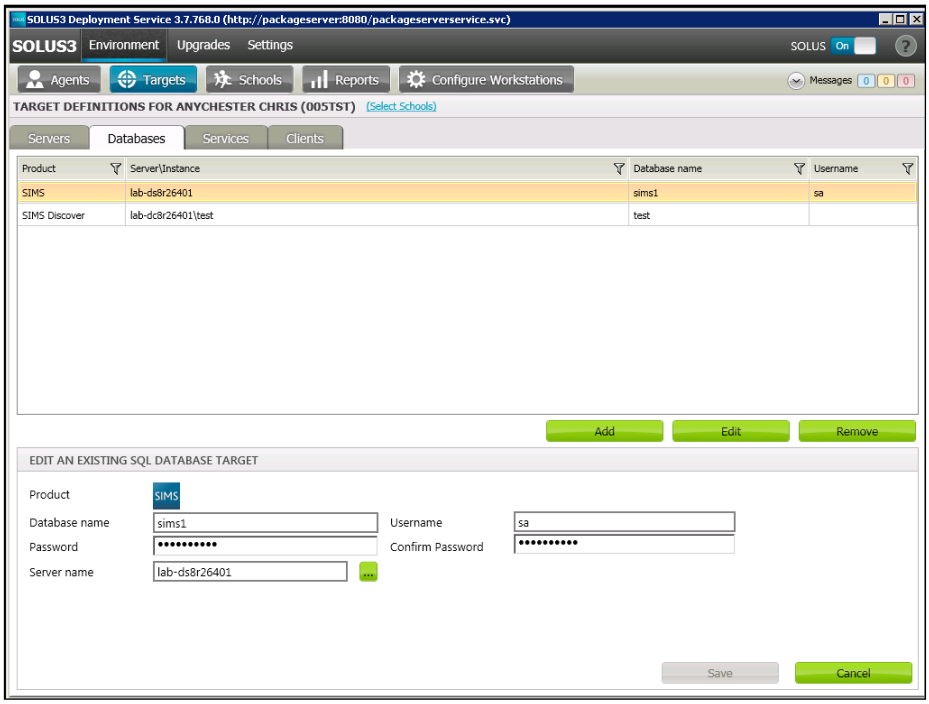
From the **Servers** tab, click the relevant server and then click the **Edit** button.

Removing a Server

From the **Servers** tab, click the relevant server, and then click the **Remove** button. You cannot remove a server if it is linked to database targets.

Databases (SIMS, FMS)

1. Select **Environment | Targets** to display the **TARGET DEFINITIONS** page.
2. Select the **Databases** tab.



Adding a Database

1. Click the **Add** button.
2. In the **DEFINE A NEW SQL DATABASE TARGET** panel, select **FMS** or **SIMS**. These products are only available if a server for these products has been defined.
3. Enter the **Database name**.
4. Enter the **Username**.
5. Enter the **Password** and **Confirm Password**.
6. To record the **Server name**, click the green **Browse** button and then select the required server.
7. Click the **Select** button to save the selection.
8. Click the **Save** button.

Editing a Database

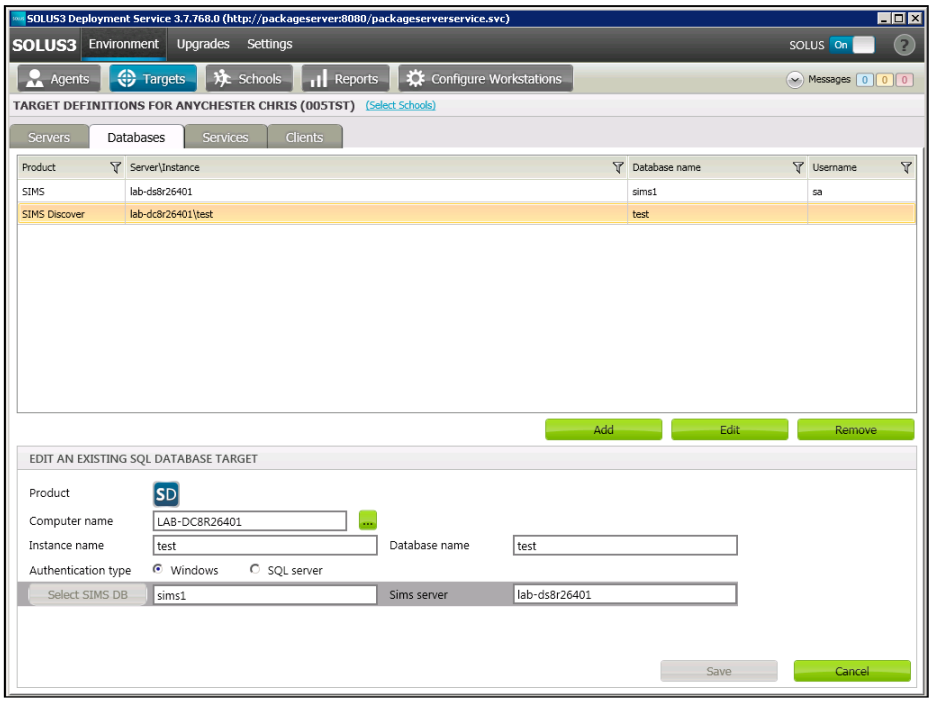
From the **Databases** tab, click the database, and then click the **Edit** button.

Removing a Database

From the **Databases** tab, click the database, and then click the **Remove** button. You cannot remove a database if it is linked to Discover targets.

Databases (SIMS Discover)

1. Select **Environment | Targets** to display the **TARGET DEFINITIONS** page.
2. Select the **Databases** tab.



Adding a Database

1. Click the **Add** button.
2. In the **DEFINE A NEW SQL DATABASE TARGET** panel, select **SIMS Discover** (SD).
3. For the **Computer name**, click the green **Browse** button and select one of the following radio buttons:
   - **Active Directory**, and then select **Domain Controllers** or **MOSS** (Microsoft Office SharePoint Server), and then click the **Select** button.
   - **Network**
   - **Agents**.
4. Select the computer name in the **AVAILABLE COMPUTERS** panel, and then click the Right-Arrow button (). This moves the selected computer(s) from the **AVAILABLE COMPUTERS** panel to the **SELECTED COMPUTERS** panel. Alternatively, search and add computers from the **SELECTED COMPUTERS** panel.

a. Enter the **Computer Name** or the **IP Address** that for which you are searching.

b. To search and add, click the **Add** button (). This button is available only if you enter a name that (partially) meets an available computer name. Wildcards cannot be used.

Adding computers in this way displays them in the **SELECTED COMPUTERS** panel with their FQDN (Fully Qualified Domain Name).

5. Click the **OK** button.
6. Enter the **Instance name**.
7. Enter the Discover **Database name**.
8. Select the **Authentication type**:
   - **Windows**

     If more than one SIMS database is defined, select the **Select SIMS database** button to select the appropriate database.
   - **SQL Server**

     a. Enter the **Username**.

     b. Enter and confirm the **Password**.

     If more than one SIMS database is defined, select the **Select SIMS database** button to select the appropriate database.
9. Click the **Save** button.

Editing a Database

From the **Databases** tab, click the database and then click the **Edit** button.

Removing a Database

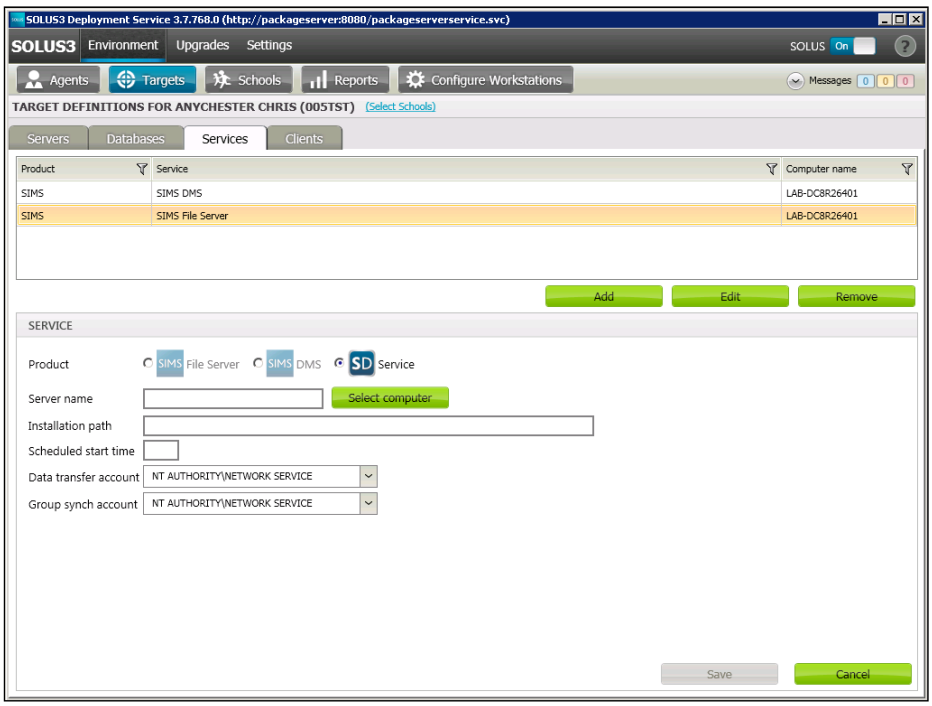
From the **Databases** tab, click the database and then click the **Remove** button. A database cannot be removed if it is linked to Discover targets.

Selecting Services

1. Select **Environment | Targets** to display the **TARGET DEFINITIONS** page.
2. Select the **Services** tab.

To add a new service:

a. Click the **Add** button to display the **SERVICE** panel.



b. Select the required service.
   - SIMS File Server SERVICE
   - SIMS DMS SERVICE
   - SIMS Discover SERVICE.

a. Click the **Save** button.

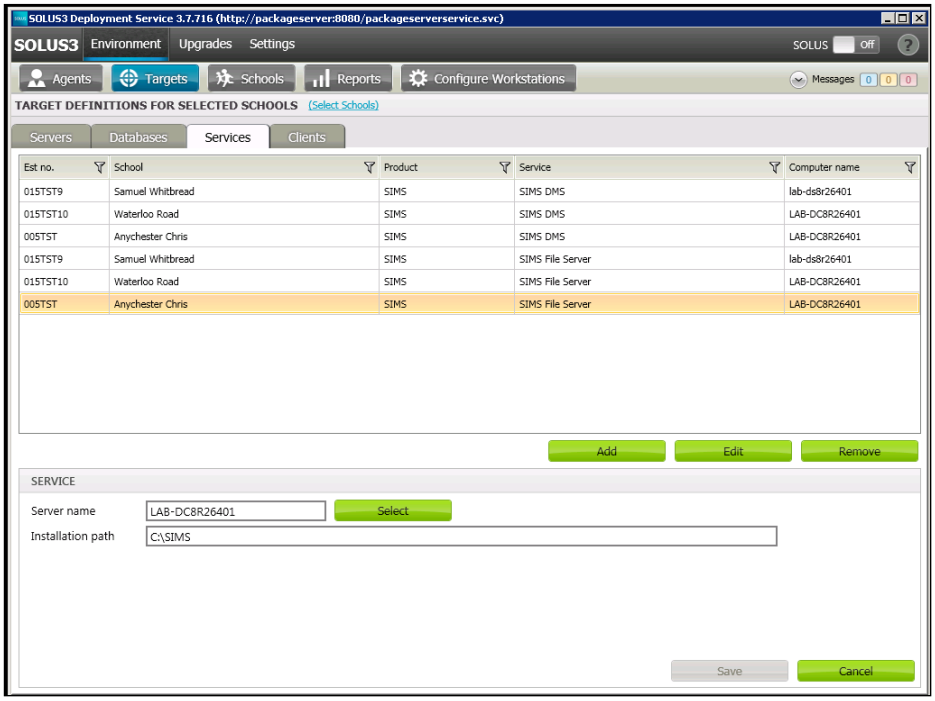
To edit a service:

a. Select the relevant service.

b. Click the **Edit** button.

c. Make the necessary changes.

d. Click the **Save** button.



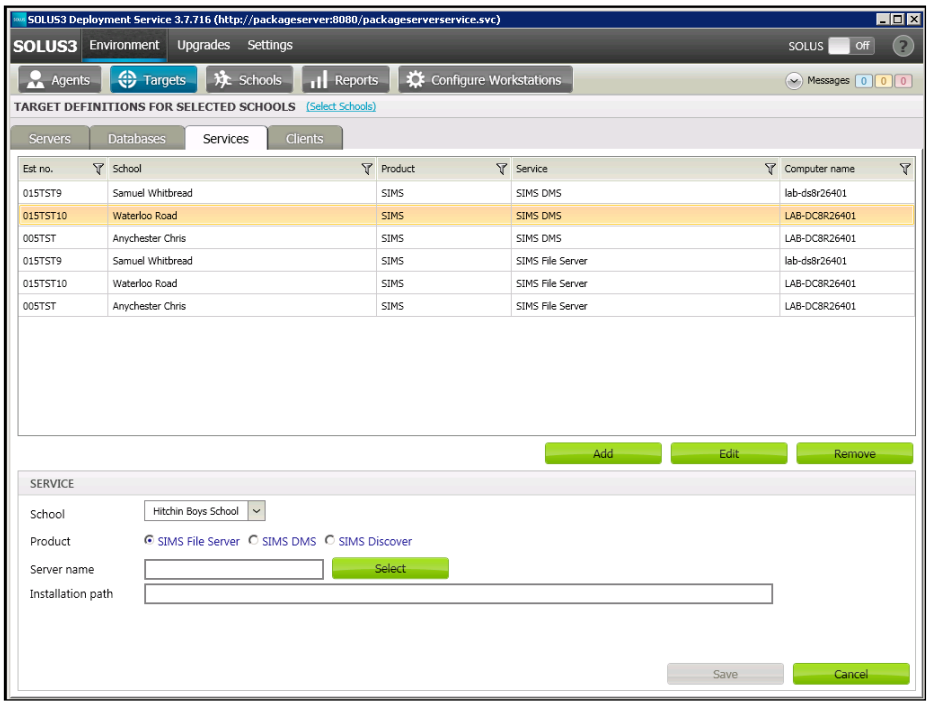
To remove a service:

a. Click the **Remove** button.

b. Click the **Yes** button to confirm removal.

The SIMS File Server Service

> *NOTE: If you have already selected and saved a server name but want to change it, click the **(Remove target)** link and then click the **Yes** button in the **Remove target definition** dialog.*



1. To record the **Server name**, click the **Select** button and select one of the following radio buttons:
   - **Active Directory**, and then select **Domain Controllers** or **MOSS** (Microsoft Office SharePoint Server), and then click the **Select** button.
   - **Network**
   - **Agents**.
2. Select the computer name in the **AVAILABLE COMPUTERS** panel and then click the right arrow button ( ). This moves the selected computer(s) from the **AVAILABLE COMPUTERS** panel to the **SELECTED COMPUTERS** panel. Alternatively, search and add computers from the **SELECTED COMPUTERS** panel.
   a. Enter the **Computer Name** or the **IP Address** you are looking for.
   b. To search and add, click the **Add** button ( ). This button is available only if you enter a name that (partially) meets an available computer name. Wildcards cannot be used. Adding computers in this way, displays them in the **SELECTED COMPUTERS** panel with their FQDN (Fully Qualified Domain Name).
3. Click the **OK** button.
4. Enter a valid **Installation path**.

> *NOTE: It is not possible to save the settings without entering the installation path.*

5. Click the **Save** button.

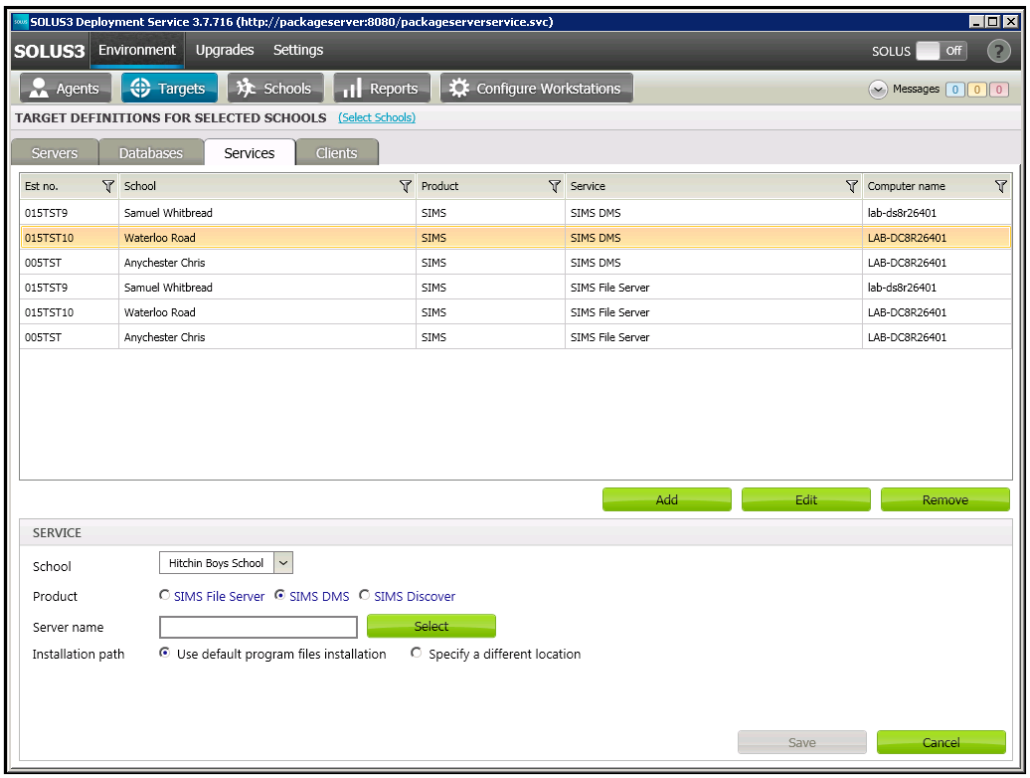
   If the services are not on a local machine, the **Domain administrator credentials** dialog is displayed.

   a. Enter the **Username** of the domain administrator.

   b. Enter and confirm the **Password** of this user.

6. Click the **Save** button.

The SIMS DMS Service



1. Click the **Add** button.
2. Select a **SIMS DMS**.
3. For the **Server name**, click the **Select** button, and select one of the following radio buttons:
   - **Active Directory**, and then select **Domain Controllers** or **MOSS** (Microsoft Office SharePoint Server), and then click the **Select** button.
   - **Network**
   - **Agents**.
4. Select the computer name in the **AVAILABLE COMPUTERS** panel, and then click the Right-Arrow button ( ). This moves the selected computer(s) from the **AVAILABLE COMPUTERS** panel to the **SELECTED COMPUTERS** panel. Alternatively, search and add computers from the **SELECTED COMPUTERS** panel.

a. Enter the **Computer Name** or the **IP Address** you are looking for.

b. To search and add, click the **Add** button ( ).

This button is available only if you enter a name that (partially) meets an available computer name. Wildcards cannot be used. Adding computers in this way displays them in the **SELECTED COMPUTERS** panel with their FQDN (Fully Qualified Domain Name).

Click the **OK** button to add the Server name.

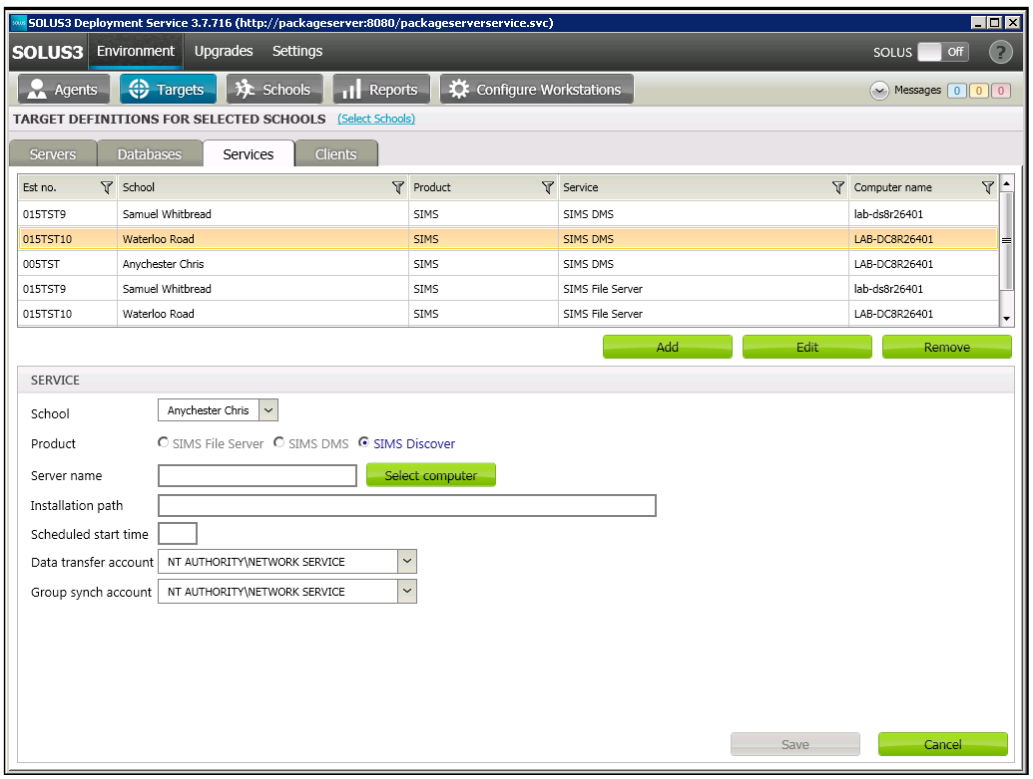
5. To record the **Installation path**, select one of the following radio buttons:
   - **Use default program files installation**
   - **Specify different location**

     Enter a valid **Installation path**. It is not possible to save the settings without doing so.
6. Complete the following steps for the **SIMS File server** panel.

The SIMS Discover Service

> *NOTE: You are required to create a Discover database target before you can setup Discover Services*

Complete the fields in this panel when installing SD services.



1. For the **Server name**, click the **Select** button, and select one of the following radio buttons:
   - **Active Directory**, and then select **Domain Controllers** or **MOSS** (Microsoft Office SharePoint Server), and then click the **Select** button.
   - **Network**
   - **Agents**.
2. Select the computer name in the **AVAILABLE COMPUTERS** panel, and then click the Right-Arrow button (). This moves the selected computer(s) from the **AVAILABLE COMPUTERS** panel to the **SELECTED COMPUTERS** panel. Alternatively, search and add computers from the **SELECTED COMPUTERS** panel.
   a. Enter the **Computer Name** or the **IP Address** for which you are searching.
   b. To search and add, click the **Add** button (). This button is available only if you enter a name that (partially) meets an available computer name. Wildcards cannot be used. Adding computers in this way, displays them in the **SELECTED COMPUTERS** panel with their FQDN (Fully Qualified Domain Name).
3. Click the **OK** button.
4. Enter a valid **Installation path**.

> *NOTE: It is not possible to save the settings without doing so.*

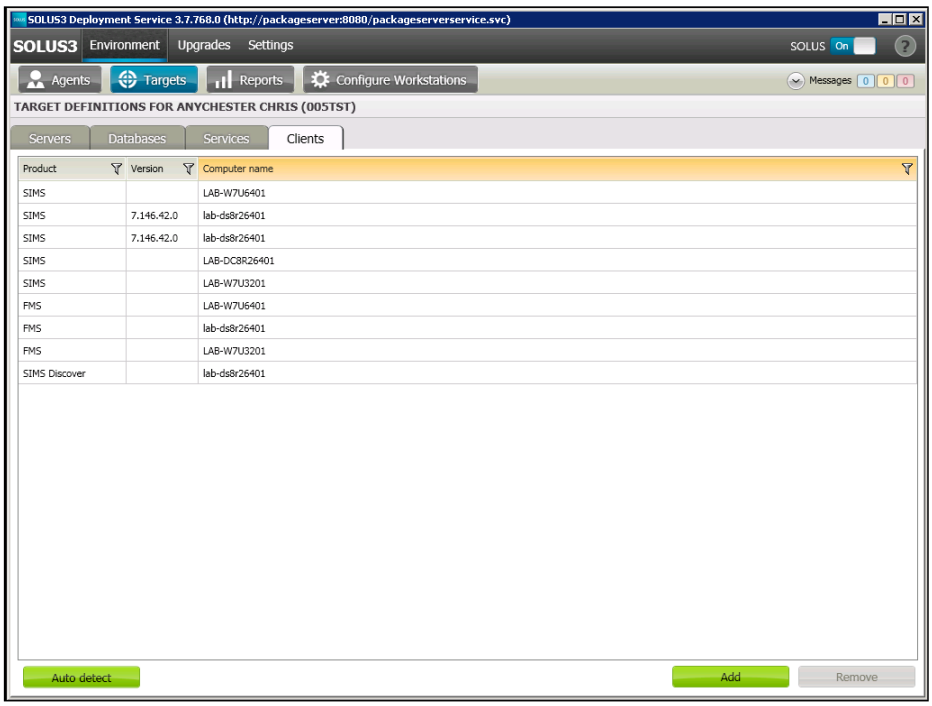
5. Enter the **Scheduled start time** in a 24-hour format.
6. Select the **Data transfer account** from the drop-down list, enter your **Domain\Username** and **Password** and then confirm your password.
7. Select the **Group synch account** from the drop-down menu.
8. Click the **Save** button.

06 Choosing how your Workstations will be Updated

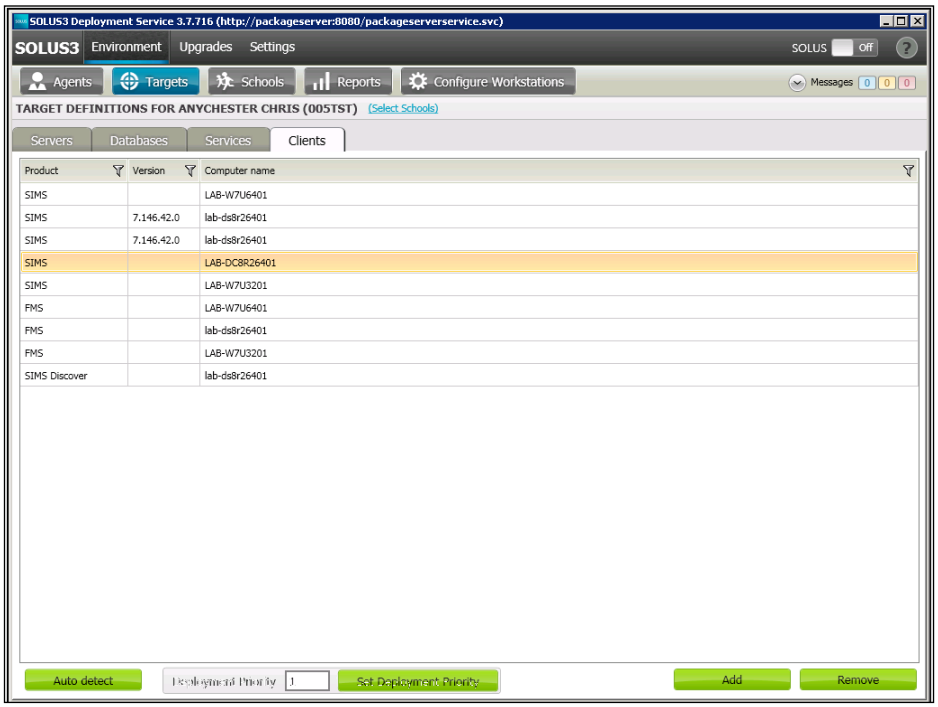
Adding Clients

1. Select **Environment | Targets** to display the **TARGET DEFINITIONS** page.

   For schools, the following **TARGET DEFINITIONS** page is displayed.



For LAs, the following **TARGET DEFINITIONS** page is displayed:

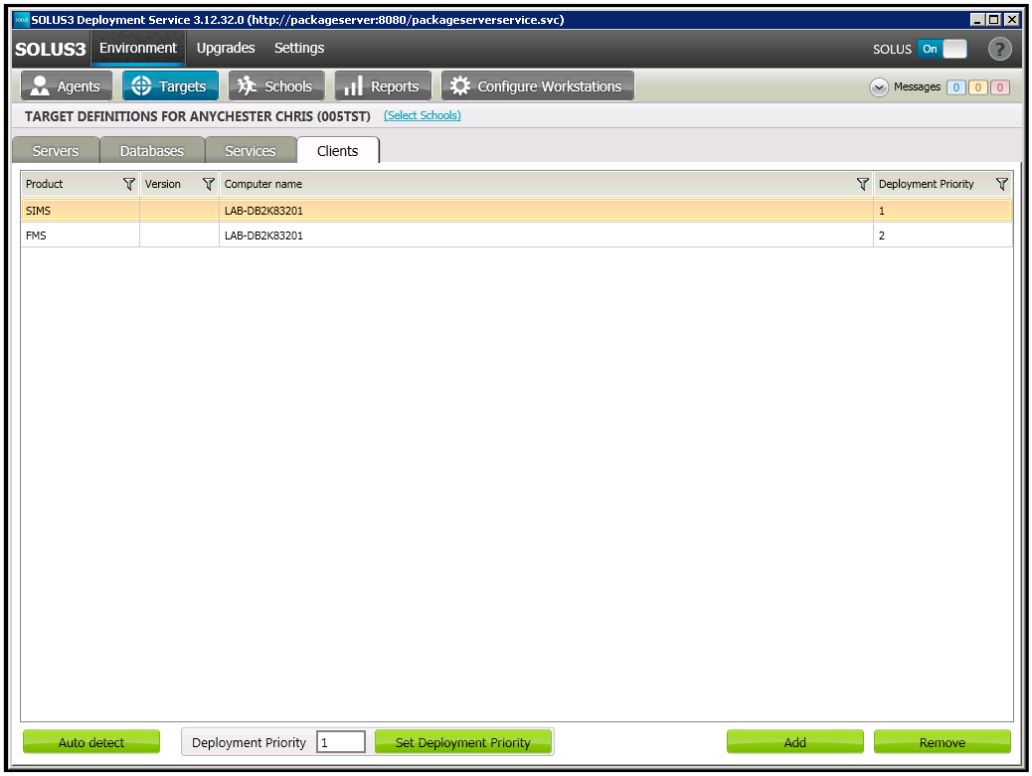


2. If you are an LA, click the **Select Schools** link to select one or more schools.

Specifying the Default Deployment Priority for an Individual Client

To ensure that updates are deployed to priority machines first, it is possible to set a deployment priority for individual clients and the products they receive. A deployment priority range can be set from 1 to 9999.

1. Select **Environment | Targets | Clients**.



2. Highlight a product/computer name combination for the relevant client.
3. Enter a priority number in the **Deployment Priority** field.
4. Click the **Set Deployment Priority** button.
5. The deployment priority specified remains the default order for subsequent updates until a different deployment priority is specified for a particular update, where applicable. If the client is subsequently deleted, their deployment priority is no longer valid.

Auto Detect

Auto detect enables you to assign SIMS or FMS clients automatically from within your environment, or from the SIMS database.

> *NOTE: If a SIMS database exists, a setup from the SIMS database populates the computer selection list automatically, based on the computers that have logged in to SIMS in the last 12 months.*

1. Select **Environment | Targets** to display the **TARGET DEFINITIONS** page.
2. Select the **Clients** tab then click the **Auto detect** button.

> *NOTE: If more than one school is selected, the **Auto detect** button becomes disabled.*

You can set up Auto detection in two ways:

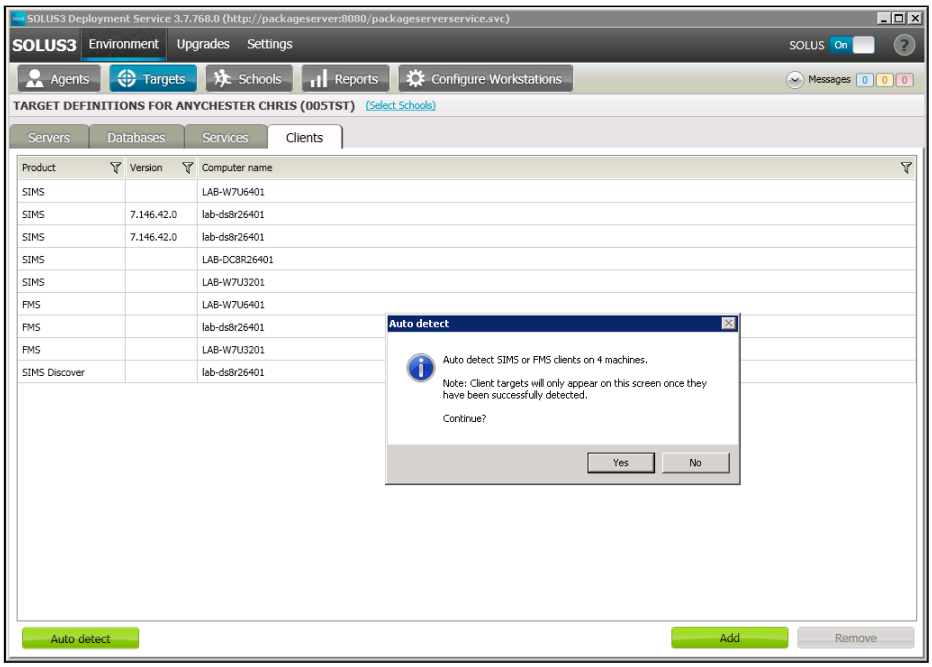
- from the SIMS database (see step 3)
- from your network environment (see step 4).

3. Select the **SIMS database** radio button.

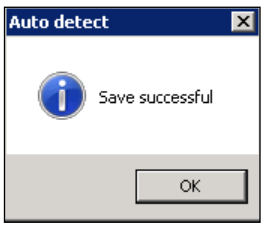
a. Enter your Domain administrator credentials.

b. Continue from step 5.

4. Select one of the following radio buttons, depending on how much of your network you want to cover:
   - **Active Directory**, and then select **Domain Controllers** or **MOSS** (Microsoft Office SharePoint Server), and then click the **Select** button.
   - **Network**
   - **Agents**
5. Select the computer name(s) in the **AVAILABLE COMPUTERS** panel, and then click the blue **Move** button. This moves the selected computer(s) from the **AVAILABLE COMPUTERS** panel to the **SELECTED COMPUTERS** panel.
6. Click the **OK** button to display the **Auto detect** dialog.



7. Click the **OK** button. SOLUS adds an agent to the selected machines and detects if SIMS or FMS is installed. The **Auto detect** dialog is displayed.



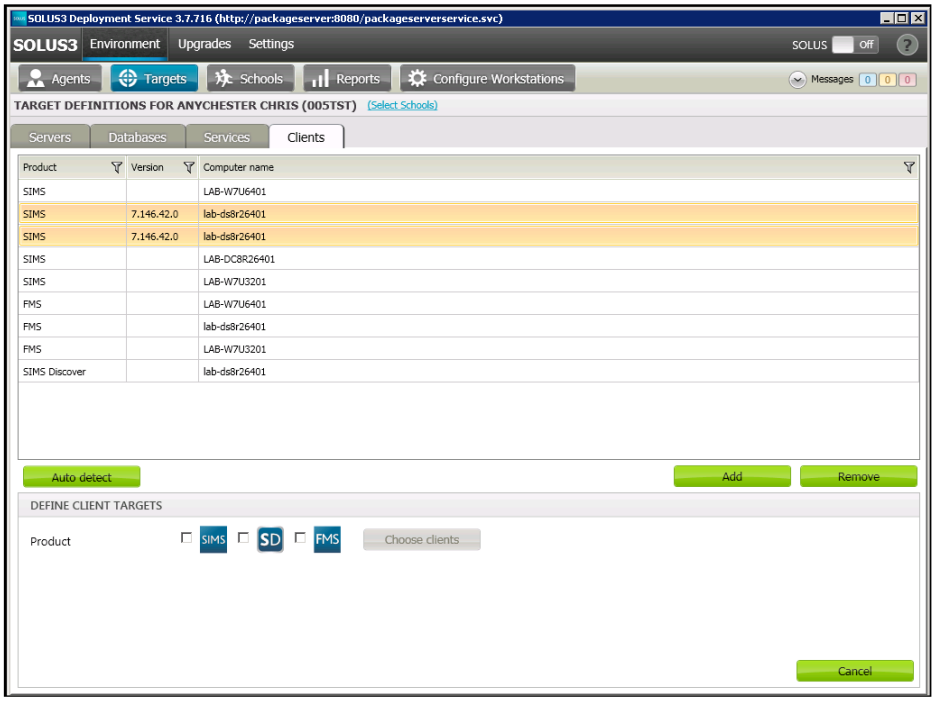
8. Click the **OK** button.

Adding Clients Manually

1. Select **Environment | Targets** to display the **TARGET DEFINITIONS** page.

> *NOTE: Clicking the **Auto detect** button enables SOLUS3 to automatically detect its clients, instead of having to define the clients manually.*

2. Select the **Clients** tab, and then click the **Add** button to add the **DEFINE CLIENT TARGETS** panel to the current page.



3. In the **DEFINE CLIENT TARGETS** panel, select one or more products using the radio buttons:
   - **SIMS**
   - **SD** (SIMS Discover)

     This option is only available after a Discover Database target has been defined.
   - **FMS**
4. Click the **Choose clients** button.
5. To select the relevant computers, click the **Select** button, and select one of the following radio buttons:
   - **Active Directory**, and then select **Domain Controllers** or **MOSS** (Microsoft Office SharePoint Server), and then click the **Select** button.
   - **Network**
   - **Agents**.

6. Select the computer names in the **AVAILABLE COMPUTERS** panel, and then click the blue **Move** button to move the selected computer(s) from the **AVAILABLE COMPUTERS** panel to the **SELECTED COMPUTERS** panel. Alternatively, search and add computers from the **SELECTED COMPUTERS** panel.
   a. Enter the **Computer Name** or the **IP Address** you are looking for.
   b. To search and add, click the **Add** button.

      This button is only selectable as long as you are typing in a name that (partially) meets an available computer name. Wildcards cannot be used however.

      Adding computers in this way, displays them in the **SELECTED COMPUTERS** panel with their FQDN (Fully Qualified Domain Name).
7. Click the **OK** button to save your selection.

   This updates the clients table and closes the **DEFINE CLIENT TARGETS** panel.

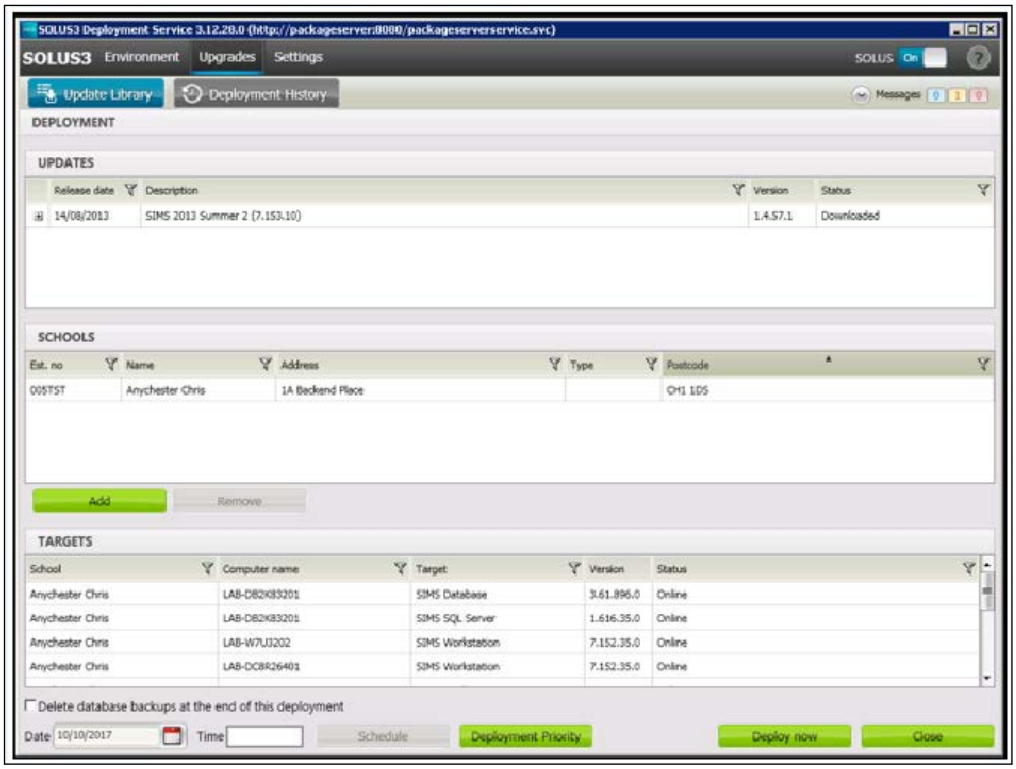
> *NOTE: If you do not select a local computer, a credentials dialog is displayed.*

Setting a Deployment Priority for a Specific Update

It is possible to change the defined deployment priority for a particular client target for a specific update and to specify a future deployment schedule via **Upgrades | Deployment History**.

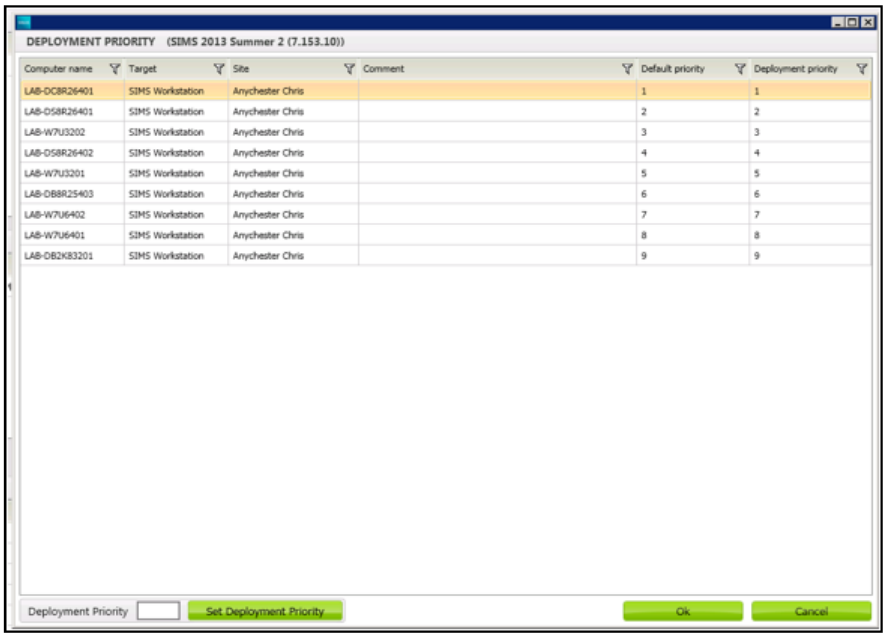
Downloaded updates available for deployment are displayed in the **UPDATES** panel of the **DEPLOYMENT** page,

1. In the **SCHOOLS** panel, select the required school name and click the **Add** button to copy the school name into the **TARGETS** panel.



All the possible targets in the school are displayed.

2. To set the deployment priority for every target in the school, click the **Deployment Priority** button to display the **DEPLOYMENT PRIORITY** dialog.



Where a default deployment priority has already been specified for a target, this is displayed in the **Default priority** column.

3. Highlight a target, enter the required **Deployment Priority** and click the **Set Deployment Priority** button.
4. Continue setting deployment priorities for all the school targets.
5. Click the **OK** button to return to the **DEPLOYMENT** page.
6. Click the **Deploy now** button or proceed to set a future deployment **Schedule**, as required. Specifying a future schedule enables you to deploy updates in priority order so that high priority targets are updated first.

07 | Alternative SOLUS3 Agent Installation Methods

Introduction

SOLUS3 installs the required agent automatically on each device that is defined on the SOLUS 3 Deployment Server UI. However, there are certain network environments where this is not possible. This chapter outlines alternative agent installation methods.

> *NOTE: Microsoft .NET Framework 4.0 Full version must be installed manually on each device that will host the DS before the installer batch files are run.*

Installing a SOLUS3 Agent using Group Policy

If there is a non-Windows firewall between the DS at the LA and devices at schools that do not have their own DS, the Windows Group Policy can be used to deploy scripts that will install the SOLUS3 agent on each device.

> *NOTE: Although Capita SIMS cannot provide bespoke scripts, using the **Export agent installer** button on the **System Configuration** page produces a default script that can then be amended.*

Any script deployed by group policy must perform the following tasks:

1. Create an installer log file name that will record installation information on each device. For example, create a file entitled `agent_install.log` in the `C:\Windows` folder of the device.
2. Run the appropriate msi installer from a network share with read access for Domain Computers.
3. Copy the following files from the folder on the DS (`C:\Program Files\Solus3\DeploymentService`)to the network share:
   - `SOLUS3AgentInstaller_x86.msi` (32-bit)
   - `SOLUS3AgentInstaller_x64.msi` (64-bit).
4. Pass the agent address to the agent installer. The default address is `net.tcp//localhost:52966`.

5. Pass the Deployment Service address to the agent installer. The default address is `net.tcp//<DS NAME or IP>:52965`. To view the DS address, select **Start | All Programs | SOLUS 3 Deployment Server UI | Settings | SOLUS3 | SOLUS**.
6. For each agent installation, pass a unique Global Unique Identifier (GUID) to the agent installer.
7. Copy the DS key file (`Solus3.Keys.DeploymentServer.Public.xml`) to the device.
8. Copy the DS key file from its default location (`C:\Program Files\Solus3\DeploymentService`) to a network share that has read access rights for Domain Computers.

Installing SOLUS3 Agents Manually

For networks that do not have a DC (domain controller), such as peer-to-peer networks, the SOLUS3 agent must be installed manually on each device (workstations and servers) in the Deployment Environment.

> *NOTE: Microsoft .NET Framework 4.0 Full must be installed on the device that will host the DS before running the installer batch files.*

- Creating the Agent Installation Files (please see *Creating the Agent Installation Files* on page *72*)
- Applying the Agent Installation Files (please see *Applying the Agent Installation Files* on page *73*).

Creating the Agent Installation Files

1. Create the installation files (please see *Creating Installation Files for a Manual Agent Installation* on page *33*).
2. Locate the batch file `Solus3AgentInstaller.bat` in the output folder, on a network drive or on removable media.
3. If required, edit the batch file to suit your installation needs. For help on batch files, please refer to Microsoft TechNet (http://technet.microsoft.com/en-us/library/bb490869.aspx).
4. Save the updated batch file.

Adding Pre-defined Agent Targets on Agent Install

1. Using Notepad (or any other plain text editor), open the `AgentInstaller.js` file.
2. Uncomment and edit the **PREDEFINEDAGENTTARGETS** parameters to include the target applications that you would like to pre-define, e.g. FMS, SIMS or `Discover`.
3. Save the file.
4. Run the SOLUS3 `AgentInstaller.bat` file to initialise the installation.
5. Once the installation completes successfully, the defined client targets are deployed.

Applying the Agent Installation Files

It is assumed that after creating the installation files, these were copied to a shared network location or to removable media.

1. Log in to the device with administrator rights.
2. Locate the agent installation files in the shared location or on the removable media.
3. Double-click the `Solus3AgentInstaller.bat` file to display the **Welcome to the SOLUS 3 Agent Setup Wizard** page.
4. Click the **Next** button to display the **End-User License Agreement** (EULA).
5. Select the **I accept the terms in the License Agreement** check box to accept the EULA.
6. Click the **Next** button to display the **Service Endpoints** page.

   The **Agent Service Address** and **Deployment Service Address** fields are populated automatically.
7. Click the **Next** button to display the **Agent Public Key** page.

   The **Public Key Path** is populated automatically.
8. Click the **Next** button to display the **Set Up Shortcuts** page.
9. Select the check boxes to indicate your shortcut preferences.
10. Click the **Next** button to display the **Destination Folder** page.
11. Use the default destination, or click the **Change** button to select a new installation location.
12. Click the **Next** button to display the **Ready to install SOLUS 3 Agent** page.
13. Click the **Install** button.
14. When the installation process is complete, click the **Finish** button.
15. Repeat this process for all devices that require the SOLUS3 agent.
16. If the machine you are adding has a SIMS application installed, SOLUS3 will automatically define a target in the Client list (**Environment | Target | Client**).

    If the machine you are adding does not have a SIMS application installed, use the **SOLUS 3 Deployment Server UI** to assign the devices target types (please see *Assigning a Target Type Manually* on page *75*).

> ***WARNING:*** *When assigning a target type to a device on which you have installed an agent manually, this device must be selected using the* ***Browse agent computers*** *button.*

Re-imaging

If your school uses imaging software such as Microsoft System Centre to enable quick re-installation of your staff workstations, SOLUS3 can be part of the image.

You will need the SIMS, FMS or Discover client to be installed on the image using the client installers from an auto-extracted SOLUS3 download file, as well as the SOLUS3 agent. The SOLUS3 agent should be installed on the image as per the manual agent installation instructions.

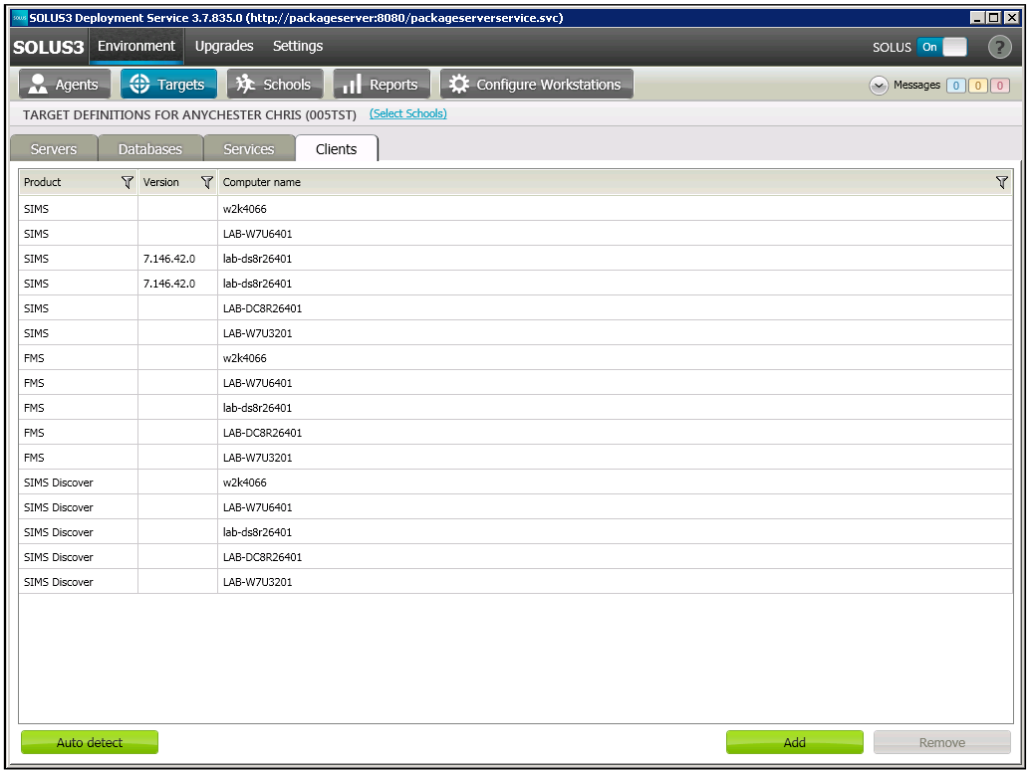
Because of the way SOLUS3 creates a unique identifier based on your hardware, a re-imaged machine will update the client details on the SOLUS3 Deployment server and you will not need to remove the old Agent entry from the DS screen.

08| Defining the Deployment Environment

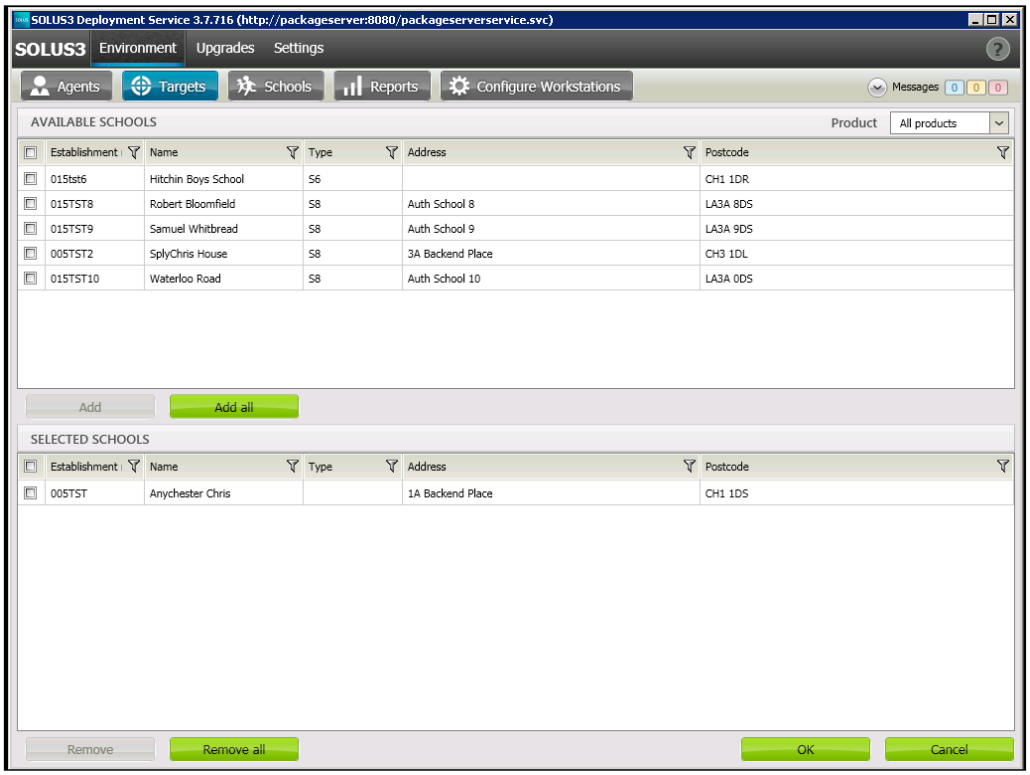
Assigning a Target Type Manually

If there are only a few computers that need to be defined for a given target type, these can be defined manually.

1. Select **Environment | Targets** to display the **TARGET DEFINITIONS** page.

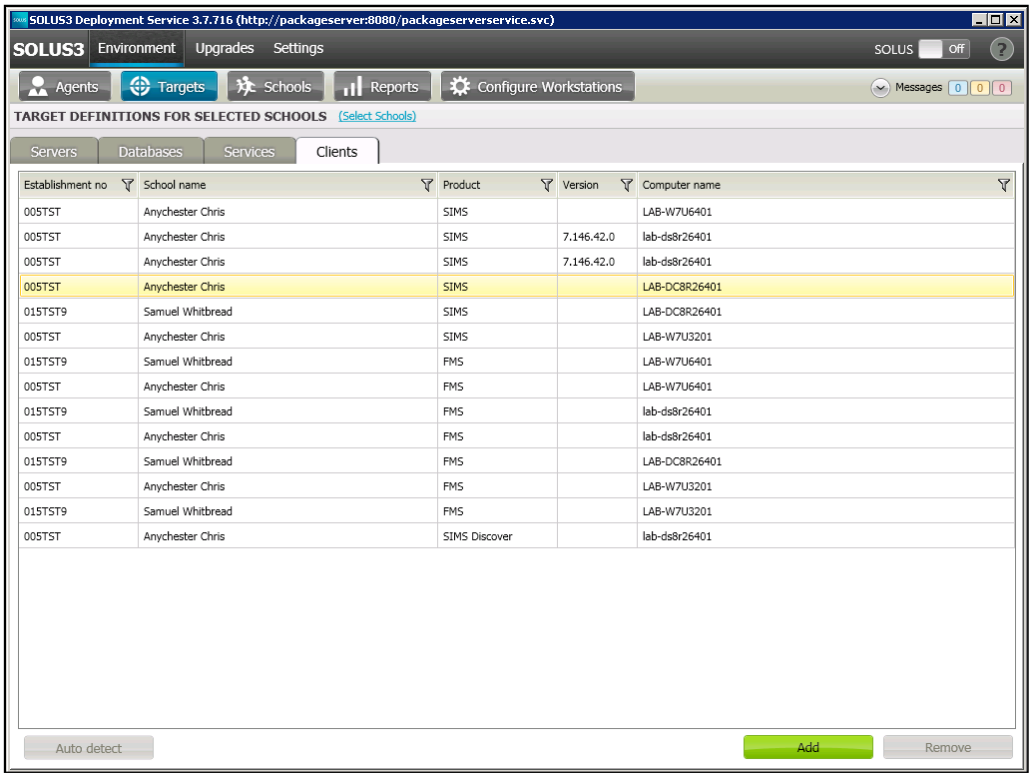


2. To change the school, click the **Select Schools** link.



3. From the **AVAILABLE SCHOOLS** panel, double-click the required school(s) to add the school to the **SELECTED SCHOOLS** panel.
4. Click the **OK** button to apply the changes.

5. Verify that the **TARGET DEFINITIONS FOR** panel now points to the newly selected school.

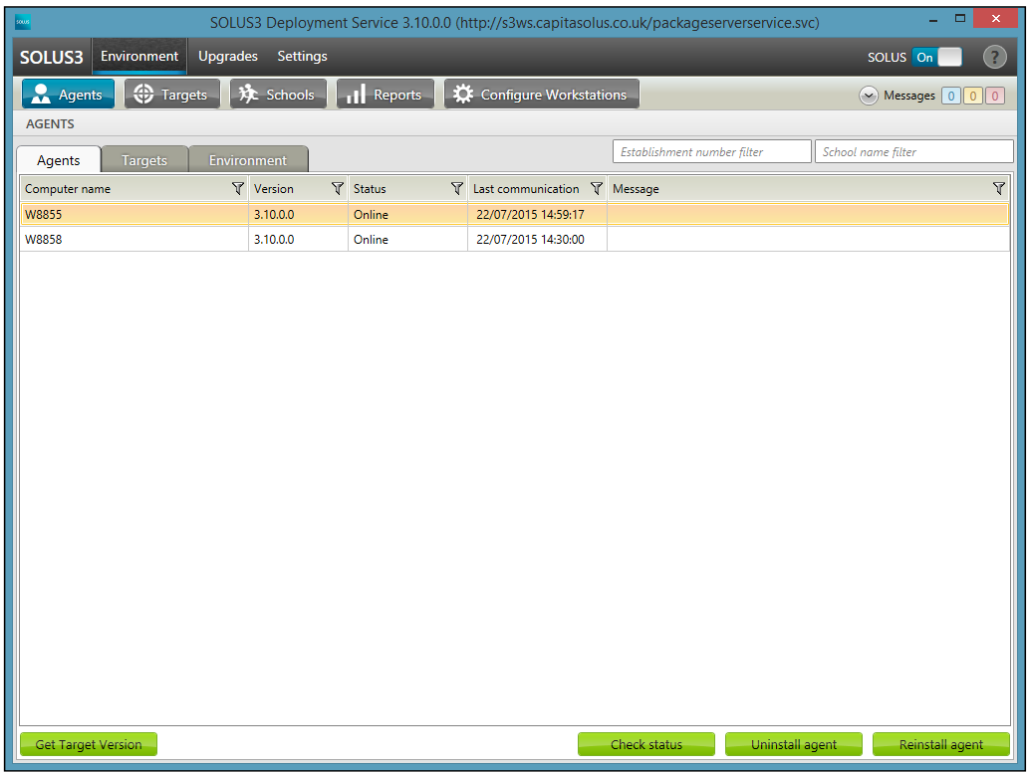


6. The **TARGET DEFINITIONS FOR ...** page has the following tabs:
   - Servers (please see *Databases (SIMS, FMS)* on page *53*)
   - Databases (please see *Databases (SIMS, FMS)* on page *53*)
   - Services (please see *Selecting Services* on page *55*)
   - Clients (please see *Adding Clients* on page *63*)

More Information:
Target Types – Required Additional Information on page *131*

Viewing SOLUS3 Agent Details

Agents reside on all the devices in the DE and tell the DS what target types exist on the device on which it is installed. Deployment Managers can view agent details to see the targets assigned to a selected device and view the deployments that have been delivered to a device.



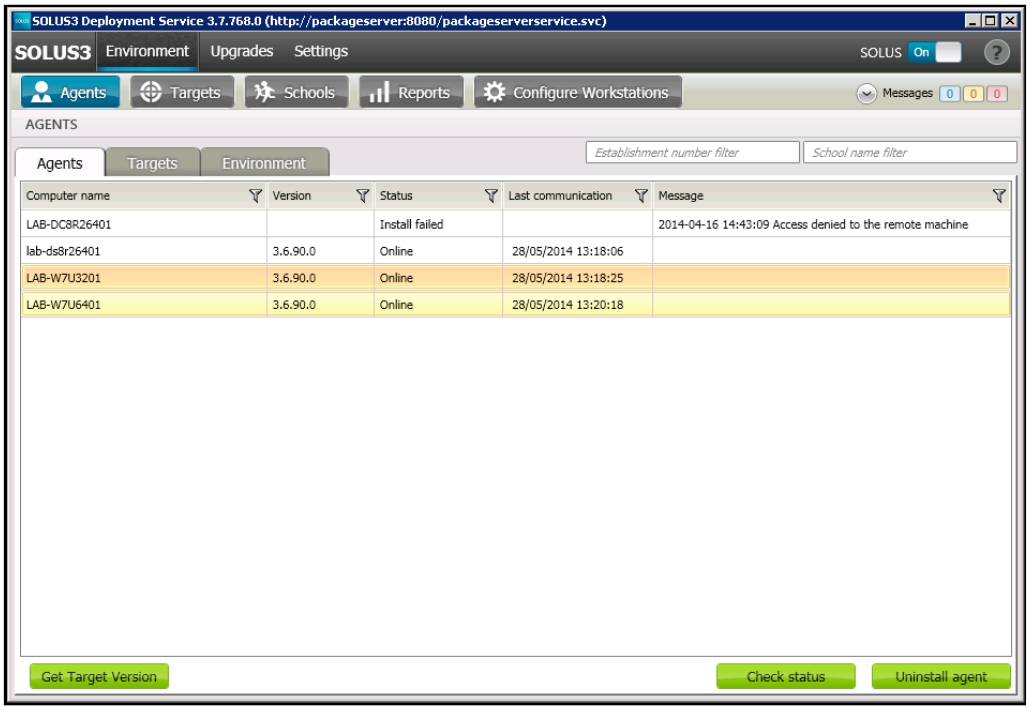
Select **Environment | Agents** to display the **AGENTS** page.

Accessing Agents Information

To display a list of devices that have the agent installed (or where an attempt has been made to install it):

1. Select **Environment | Agents** to display the **AGENTS** page.

2. Select the **Agents** tab to display the computers on which SOLUS has been installed.



This tab displays the following columns:

- **Computer name**
- **Version** - the SOLUS agent version installed on the target.
- **Status** - Online, Offline, Install failed, and so on.
- **Last communication** - the name of the site for which the target has been defined.
- **Message**

3. In the **Computer name** column, select one or more computers.

> *NOTE: The on-screen information is refreshed periodically, based on the heartbeat.*

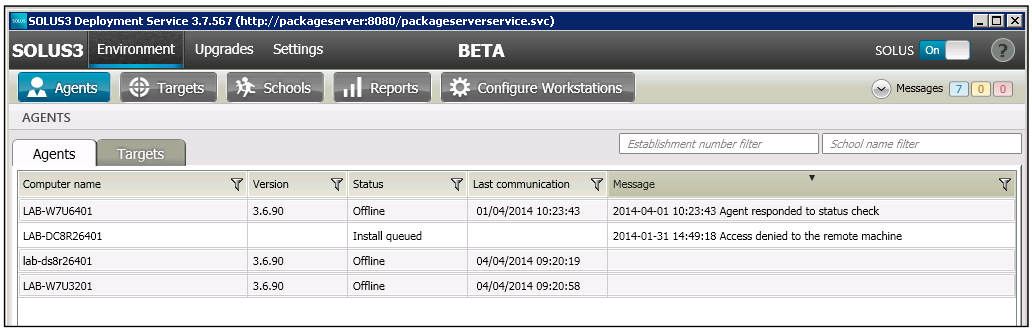
- Click the **Get Target Version** button to update the version in the target tab. The **Version** column displays the updated target version.
- Click the **Check status** button to update status and last communication status. The **Status** column displays the updated status.

Checking the Agent Status

To verify that an Agent is online, a request can be sent to the agent.

1. Select **Environment | Agents** to display the **AGENTS** page.

2. Select the **Agents** tab to display a list of devices with an agent installed.



3. In the **Computer name** column, select one or more computers and then click the **Check status** button.

   SOLUS displays the message **An agent status check request has been sent to the selected agents**.

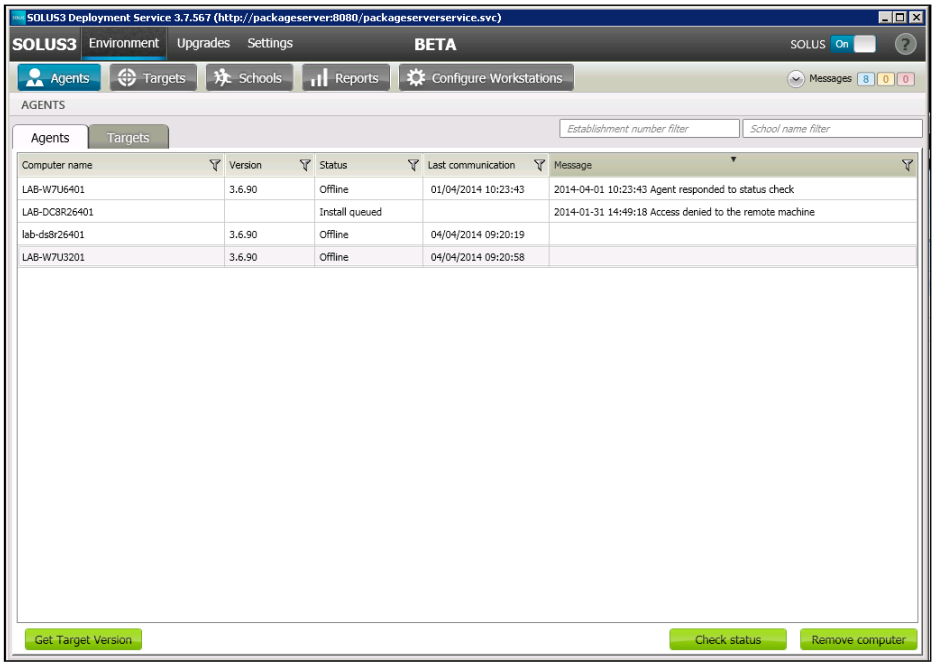
   The status is displayed in the agent's **Message** column.

> *NOTE: All agent responses are subject to network traffic speed.*

Performing a Target Type Version Check

To check target versions manually, a request can be sent to the agent.

1. Select **Environment | Agents** to display the **AGENTS** page.
2. Select the **Agents** tab to display a list of devices with an agent installed.



3. In the **Computer name** column, select one or more computers and then click the **Get Target Version** button.

   SOLUS displays the message **A request has been sent to retrieve selected agent target versions**.

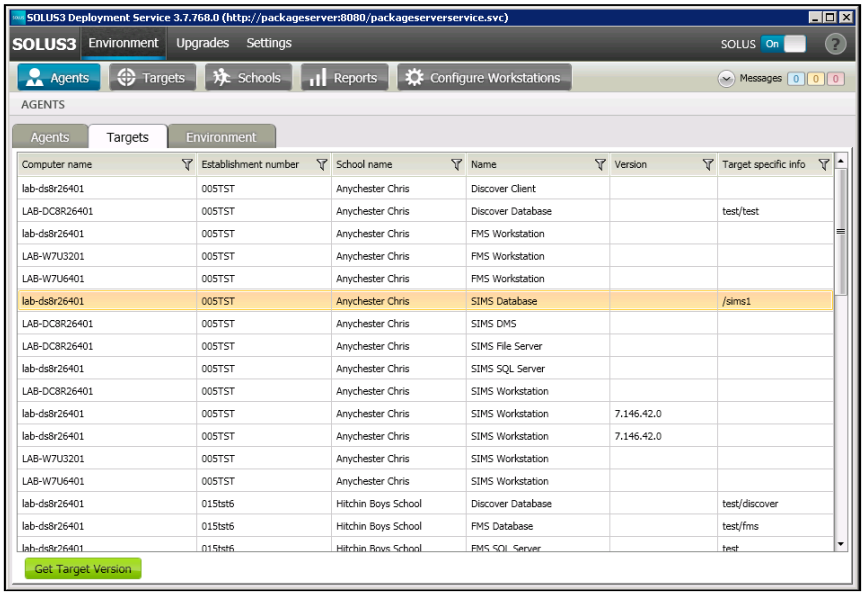
The **Version** column displays the updated target version.

> *NOTES: All agent responses are subject to network traffic speed.*
>
> *When you want to remove an agent/device, the target type definition must be removed first, otherwise Target Type Version Check will attempt to download and deploy updates.*

Accessing Targets Information

To display a list of targets:

1. Select **Environment | Targets** to display the **TARGETS** panel.
2. Select the **Targets** tab.



This tab displays the following columns:

- **Computer name**
- **Establishment number** - the number of the site for which the target has been defined.
- **School name** - the name of the site for which the target has been defined.
- **Name**- the name of the target.
- **Version**- the software version installed on the target.
- **Target specific info**

3. In the **Computer name** column, select one or more computers.
4. Click the **Get Target Version** button for the **Version** column to display the updated target version.

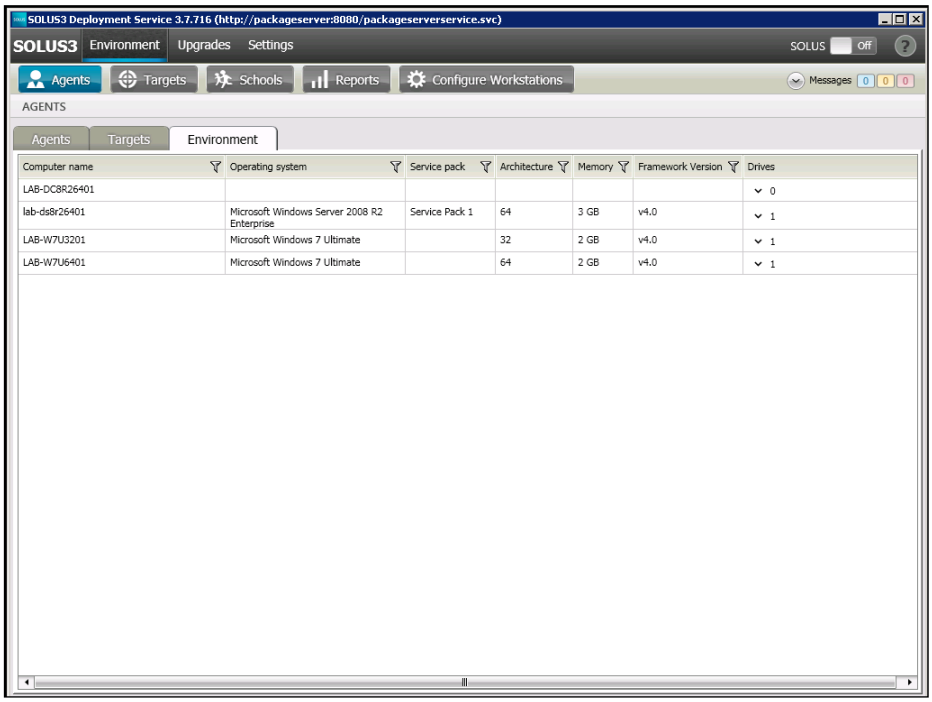
> *NOTE: All agent responses are subject to network traffic speed.*

Accessing Environment Information

This page provides concise system details. All output is on-screen only.

To display a list of targets:

1. Select **Environment | Agents** to display the **AGENTS** page.
2. Select the **Environment** tab.



This tab displays the following columns:

- **Computer name** - the computer name as set in Microsoft Windows.
- **Operating system** - the operating system of the workstation that the agent is installed on.
- **Service pack** - the service pack of the installed operating system.
- **Architecture** - 32-bit or 64-bit.
- **Memory** - the amount of installed RAM.
- **Framework version** - the version of Microsoft .NET Framework installed on the device.
- **Drives** - this field contains a drop-down list that provides access to:
  - Number of drives
  - Disk Drive letter(s)
  - Disk Space Available.

Sorting and Filtering Data

- With the exception of the **Drives** column, you can filter on all columns.
- With the exception of the **Drives** column, you can sort on any column.

Cancelling a Pending SOLUS3 Agent Installation

If a target type has been assigned to a device, but the Agent status is **Install queued**, a Deployment Manager can cancel the agent installation as follows:

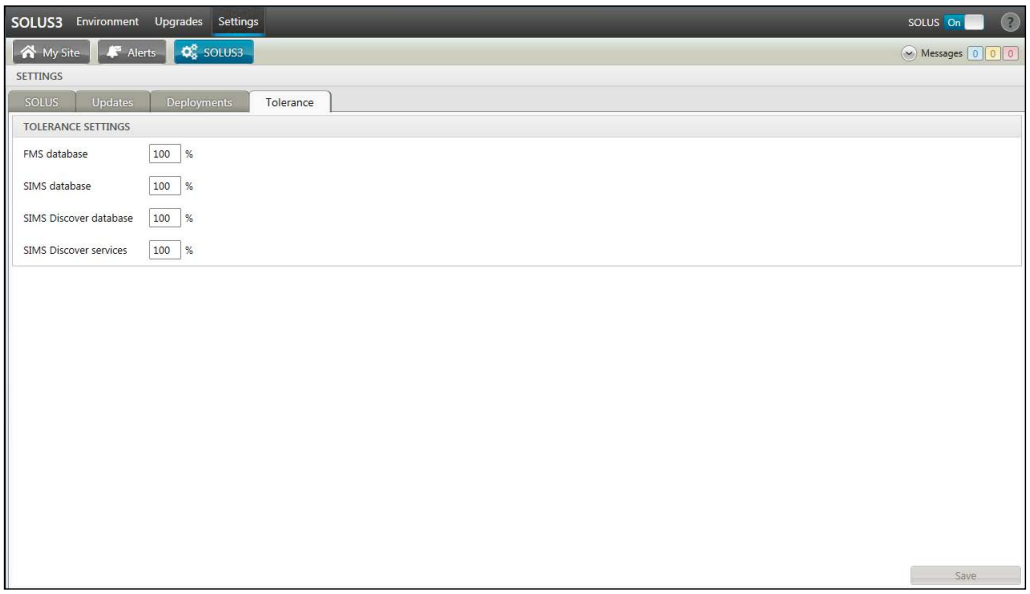
1. Select **Environment | Agents** to display the **Agents** page.
2. Select the **Agents** tab to display a list of devices with an agent installed.
3. Select the names of the devices to which you no longer want to install the agent.
   - Use **Ctrl + Click** to select individual devices.
   - Use **Shift + Click** to select a range.
4. Click the **Cancel installation** button on the navigation bar.
5. When prompted, click the **Yes** button to confirm the cancellation of the installations.

Configuring Tolerance Settings

This function is used to determine if a partially failed upgrade should be rolled back.

> *NOTE: Tolerance settings are relevant only to LAs.*

The tolerance percentage defines the percentage of computers/devices that must be upgraded successfully for a deployment to be considered successful and not to be rolled back.



For example:

- A tolerance of 100% means that all deployments for that target type must be successful, otherwise SOLUS3 will attempt to roll back all devices to their previous state.

- A tolerance of 80% would mean that maximally 20% of deployments could fail before the operation is considered unsuccessful and a rollback is attempted.

Considerations:

- The number of targets that must be deployed successfully is rounded up.

  If five SIMS SQL databases are to be updated and the tolerance is 50%, then three targets must be updated successfully for the deployment to be considered successful.

  Deployment Managers must carefully consider target tolerance settings, particularly in hosted environments.

  If an LA hosts 100 SQL Servers, to roll back 99 successful upgrades because one update failed would be undesirable. Decide on the tolerance levels that you can be comfortable with, if it comes to rolling back successful installations.
- Rollback will not be attempted if the Deployment Manager has deselected the **Roll back deployment on failure** check box on the **Settings** page (please see *Accessing Agents Information* on page *78*).
- Tolerances can only be set for database targets, such as SQL servers. SIMS workstations cannot have a tolerance set. If a SIMS workstation is updated successfully, it will not be rolled back regardless of how many other SIMS workstation updates are unsuccessful.
- Tolerance levels are calculated based on the number of targets that are online at the time the deployment is run, not the total number of defined targets. If 10 SIMS SQL Servers are defined in the DS, but only eight are online at the time a deployment is attempted, then success is eight successful deployments (assuming a default 100% tolerance for SIMS SQL Servers).
- Tolerance settings are not site-specific.

  An LA that hosts the SIMS SQL database for all schools in the LA will only have to change the tolerance for that target type once. The change will apply to all the SIMS SQL databases hosted by the LA.

1. Select **Settings | SOLUS3** to display the **SETTINGS** page.
2. Select the **Tolerance** tab to display the **TOLERANCE SETTINGS** panel.
3. Edit the following tolerances, if required.
   - FMS database
   - SIMS database
   - SIMS Discover database
   - SIMS Discover services

   The default values are set to **100**%.
4. Click the **Save** button.

Removing SOLUS3 Agents and Devices

There may be occasions where it is necessary to remove an agent or device manually. In some cases, this may be a prerequisite for re-installing an agent.

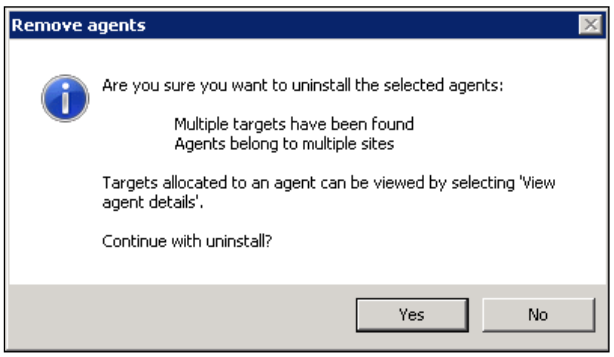
Removing an Agent from a Device

If you experience repeated failed client installation for the same computer, it may be necessary to remove the SOLUS3 agent from a device before attempting a new installation.

1. Select **Environment | Agents** to display the **AGENTS** page.
2. Click the **Agents** tab.
3. Select the name of the device(s) from which you want to remove the agent.
4. Click the **Uninstall agent** button.

   The following scenarios apply:

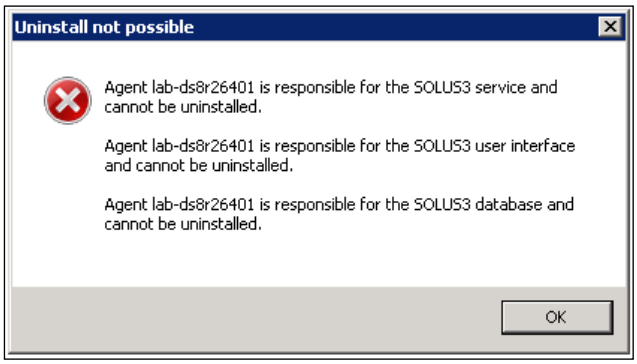
   a. The agent can be removed.



   This message is for information only. It reminds you of the consequences of agent removal but will allow you to continue.

   - Click the **Yes** button to remove the computer.
   - Click the **No** button to cancel removal.

   b. The agent cannot be removed.



   This error message stops you removing the computer.

   - Click the **OK** button to close the message.
   - Click the Windows close button (x) to close the message.

Removing a Device

If a device is no longer on the network, it makes sense to remove this device for the SOLUS3 environment. Similarly, if an installation has failed, and there will be no attempt at a re-installation, you may wish to remove the device from the SOLUS3 environment. This action keeps your system tidy, maximises security and avoids confusion.

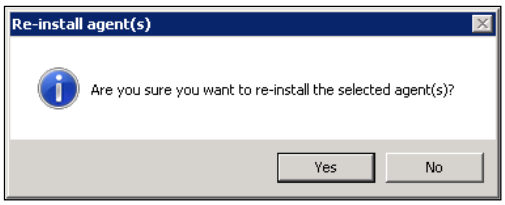
1. Select **Environment | Agents** to display the **AGENTS** page.
2. Select the **Agents** tab.
3. Select the name of the device(s) from which you want to remove the agent.
4. Click the **Remove computer** button to display the following message.

   This message is for information only. It reminds you of the consequences of the removal of the computer, but enables you to continue anyway.
5. Click the **Yes** button to remove the computer from the environment.

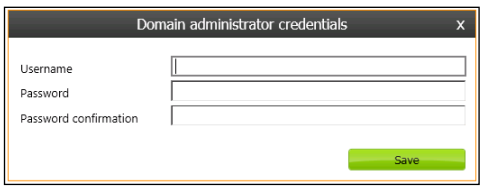
Re-installing an Agent on a Device

Agents can be re-installed on devices that have previously had an agent installed. If an agent has become corrupted, it is possible to re-install on a device at any time.

1. Select **Environment | Agents** to display the **Agents** page.
2. Select the **Agents** tab.
3. Select the name(s) of the device(s) on which you want to re-install the agent.
4. Click the **Reinstall agent** button to display the **Re-install agent(s)** dialog.



5. Click the **Yes** button to start the re-installation process and to display the **Domain administrator credentials** dialog.



6. Enter the **Username**.
7. Enter and confirm the **Password**.
8. Click the **Save** button.

09 | Managing Updates

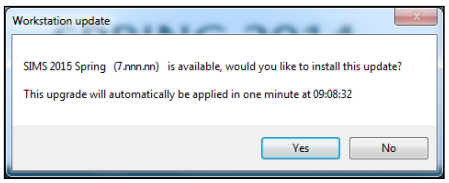
Introduction

After defining the Deployment Environment (DE) and installing agents, the Deployment Service (DS) can begin to download and deploy updates. After the initial setup is complete, updating devices is a four-step process:

1. Check for new updates.
2. Download updates to the Update Repository.
3. Deploy updates to agents on devices.

> ***WARNING:*** *When a SIMS or FMS upgrade is run using SOLUS3, any open instance of that software on that machine will be closed automatically. This action enables SOLUS3 to continue its upgrade. If the software is not closed, the files will be locked by the operating system and this can prevent the upgrade from running.*

If you are running SOLUS 3.8 (or later) and the SIMS 2014 Autumn Release (or later), and you attempt to run SIMS or FMS and the version of the client does not match that of the corresponding database, SOLUS identifies this and offers the you the option of carrying out the upgrade now or at a later date.



If no input within a minute, the upgrade occurs automatically.

To run the client upgrade before the minute is up, click the **Yes** button.

If you do not wish to run the upgrade now, click the **No** button. SIMS will attempt to open but will probably be given a database incompatibility error. Next time you run SIMS, you will be prompted to run the upgrade again.

This chapter details the necessary steps to deploy updates.

NOTE: Deployment Services send non-sensitive information regarding updates to Capita SIMS.

- The information sent relates only to the download of an update and deployment status of an update for a particular DS.
- The information sent to Capita SIMS contains no more information than the information previously sent from sites using SOLUS2.

Enabling SOLUS3 to Deploy Updates

Before enabling SOLUS3 to deploy updates, ensure that you carry out the following processes.

- Define your Deployment Environment.
- Back up the solus3_deployment_server database.

After enabling SOLUS3, updates are deployed according to the deployment plans created by the Deployment Manager. This process needs to be completed only once, unless the Deployment Manager disables SOLUS3.

To enable SOLUS3 and deliver updates to the agents:

1. Click the **SOLUS** button at the top right-hand side of any SOLUS page to display the **Enable SOLUS3** dialog

2. Click the **Yes** button to confirm your selection and update the status.

IMPORTANT NOTE: *Continue to back up the* `solus3_deployment_server` *database on a regular basis.*

Viewing Update Details

Information relating to any available update can be viewed by the Deployment Manager. The information that can be displayed includes updates, dependencies, affected target types, deployments that have included the update and the schools to which the update has been authorised. This information can be useful when planning deployments.

1. Select **Upgrades**.
2. Click one of the following buttons:
   - Update Library (please see *Update Library* on page *89*)

     This enables you to download and distribute updates.
   - Deployment History (please see *Deployment History* on page *96*)

     This enables you to plan and verify deployments.

Update Library

The DS downloads a list of available updates automatically. You can check for new updates manually.

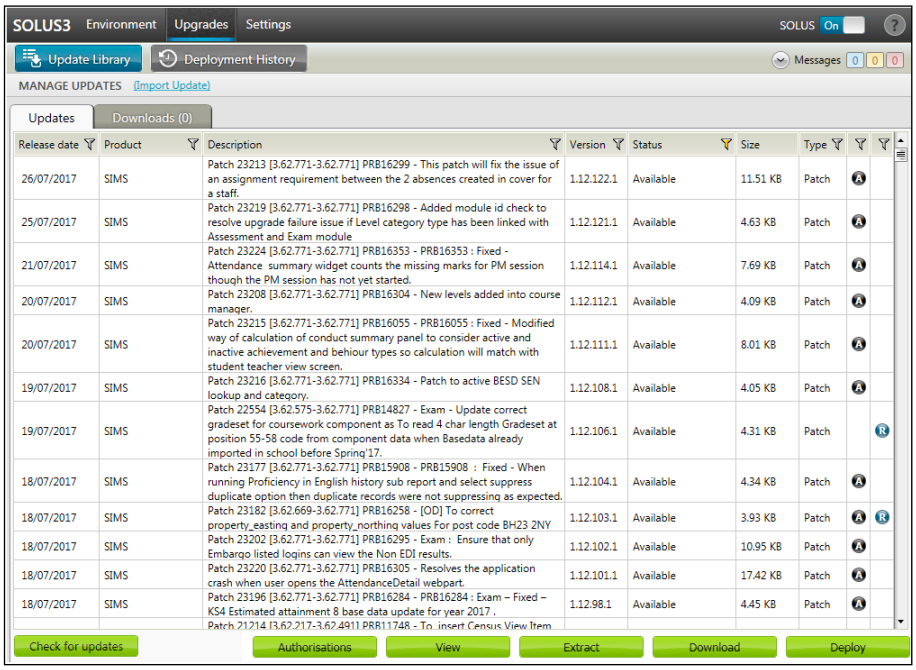
Select **Upgrades | Update Library** to display the **MANAGE UPDATES** page. Note the link **(Import Update)** to update the library from removable media, such as CD.

Checking for Updates

To check for updates manually:

1. Select **Upgrades | Update Library** to display the **MANAGE UPDATES** page.
2. Select the **Updates** tab.

   This tab provides a list of applicable updates, and information relating to these updates.



At the end of each row, an **A** indicates that the update can be auto-deployed and an **R** in the adjacent column will be present if the update can be deployed multiple times at the school.

Click the **Check for updates** button to refresh the updates page. This enables you to verify if any new updates are authorised. The message **Connecting to the CCS update server for new updates** is displayed. The DS contacts the Capita SIMS servers to find available updates and the content of the table is updated.

> *NOTE: One or more updates may have been withdrawn by Capita SIMS or by your LA. The status of an update then changes to* ***Withdrawn****. Withdrawn updates cannot be deployed.*

3. Select one or more update(s) from the list.

   One or more buttons become available at the right-hand bottom side of the panel:

   - Authorisations (this applies to LAs only)
   - View (please see *Viewing Update Details* on page *90*)
   - Extract (please see *Extracting Updates* on page *91*)
   - Download (please see *Downloading Updates* on page *91*)
   - Deploy (please see *Deploying Updates* on page *105*).

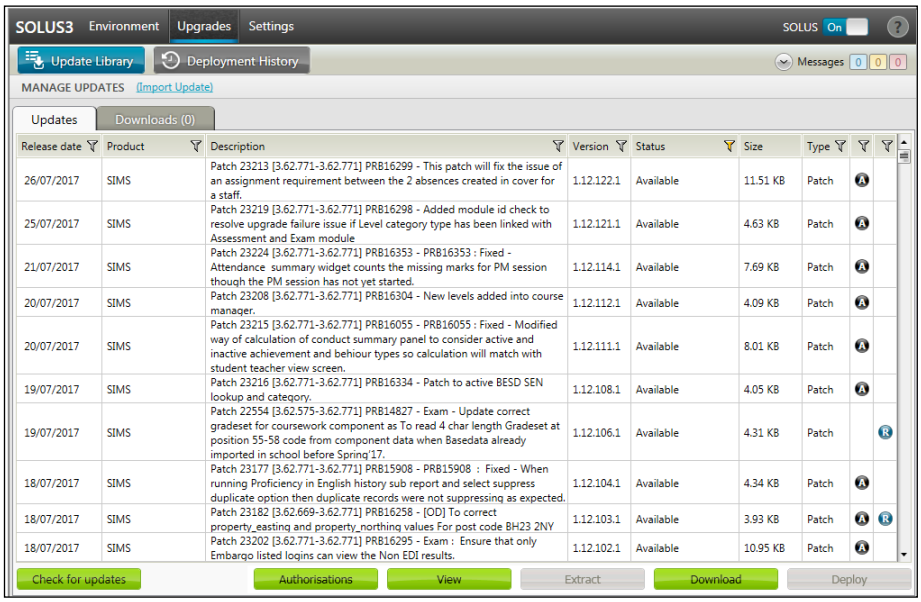
Viewing Update Details

Click the **Update Library** button to display the **MANAGE UPDATES** page. At the top of the page, SOLUS displays the columns:

- **Release date**
- **Product**
- **Description**
- **Version**
- **Status**
- **Size**
- **Type**

The default view for a school will only display the updates that the school require, based on their current software. It is possible to view other available updates by clicking the **Check for updates** check box at the bottom left of the **MANAGE UPDATES** page.

To view dependencies for this update, click the plus button on the left-hand side. To collapse this information, click the minus button.



Targets

The **Targets** tab displays the following columns:

- **Name**

  The name of the target that the update will be deployed to, e.g. Solus 3 Agent, Solus 3 Database, Solus 3 Deployment Service, Solus 3 GUI (Graphical User Interface).

- **Number of possible targets in environment**

  The total number of targets with this target type assigned in the DE (Deployment Environment)

To view dependencies for this update, click the plus button on the left-hand side. To collapse this information, click the minus button.

You can sort the content on any column.

Click the **Back** button to return to the previous page.

Downloading Updates

Select the required product(s) from the **UPDATES** tab and then click the **Download** button.

- SOLUS queues the selected product(s) for download to add it to your local software library.
- The **Status** column indicates:
  - **Available**
  - **Download queued**
  - **Downloaded**
  - **Downloading**
  - **Withdrawn** (this indicates that Capita SIMS or your LA has withdrawn an update)
  - **Download failed**.
- The number in the **Downloads (**n**)** tab is incremented (where n is the number of downloads).

When the download of an update has finished:

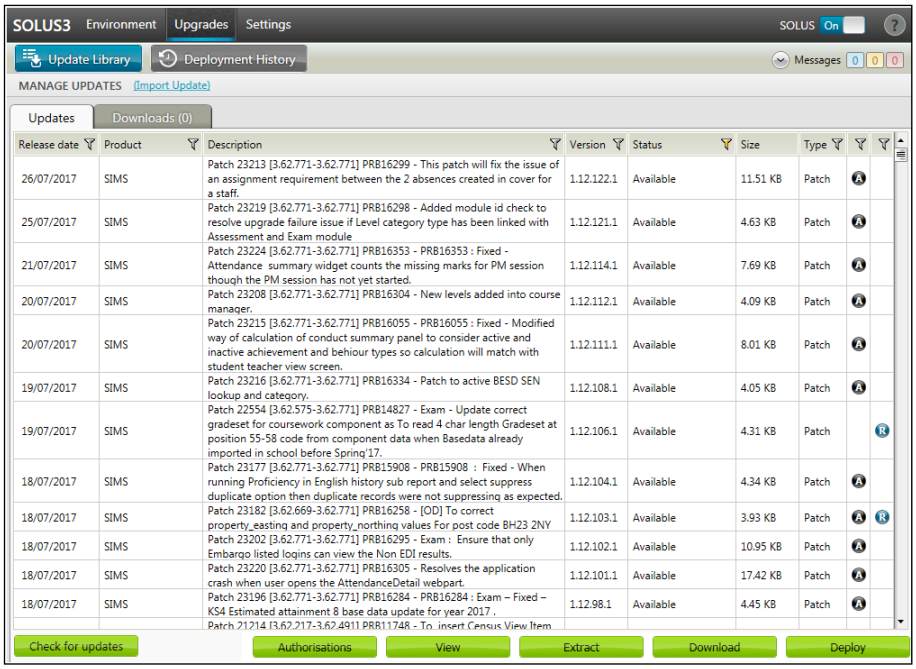
- in the **Downloads** panel, the item is removed from the queue.
- in the **Updates** panel, the **Status** of the item changes to **Downloaded**.

Extracting Updates

If you want to extract the installers for a particular package (e.g. `SIMSApplicationSetup.exe` for a SIMS release) and the extraction process has not been set up to run automatically, the following manual process can be run. Information on how to set SOLUS up to extract update packages automatically is also available (please see *Configuring Software Update Downloads* on page *45*).

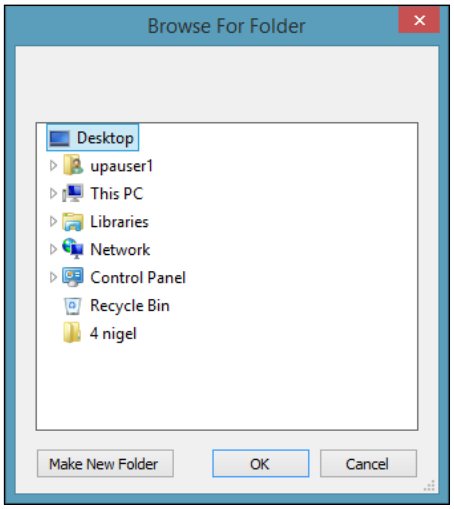
1. Select **Upgrades | Update Library** to display the **MANAGE UPDATES** page.
2. Select the **Updates** tab.

This tab provides a list of applicable updates, and information regarding them.



> ***IMPORTANT NOTE:*** *Prior to extraction, the update package must first be downloaded (please see* Downloading Updates *on page* 91*).*

3. Highlight the package(s) you want to extract.
4. Click the **Extract** button to display the **Browse for Folder** dialog.



5. Navigate to the required location. If the required location does not exist, click the **Make New Folder** button and enter a suitable name.
6. Click the **OK** button.

Managing Downloads

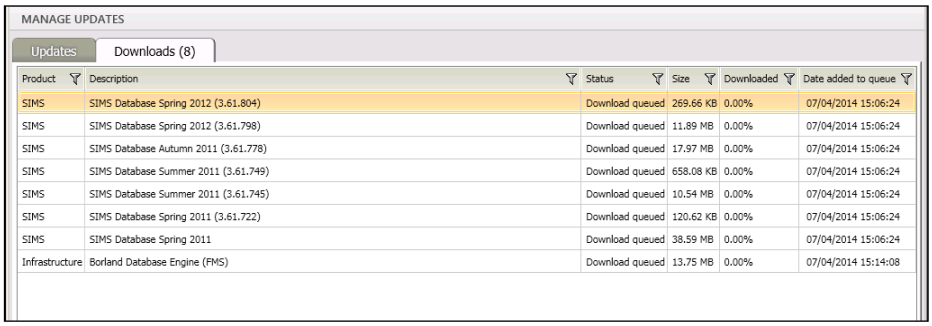
When the DS downloads an update to the Update Repository, the files are placed in the Update Repository for the DS. In some DEs, downloading updates to the repository may not be necessary. For example, in an Authorising LA model, where each school has its own DS and Update Repository, the LA would not necessarily download all updates to its Update Repository. However, each school would have to download the updates from Capita SIMS to its school Update Repository.

1. Select **Upgrades | Update Library** to display the **MANAGE UPDATES** page.
2. Select the **Downloads** tab to display a list of all the items that have been queued for download at the top of the panel; the details for each item you select are shown at the bottom of the panel.

Queued for Download

The upper part of the **Downloads (**n**)** tab displays a table containing all items that have been queued for downloading (where n is the number of queued downloads).

The following graphic is for representation purposes only.



The **Downloads** tab in the **MANAGE UPDATES** page displays the following columns:

- **Product** - general product category
- **Description** - full product name and version
- **Status** - **Available**, **Queued** or **Downloaded**
- **Size** - file size in megabytes
- **Downloaded** - download percentage completed.
- **Date added to queue** - date the item was added to the download queue. This is not affected by pausing and resuming the download.

Items Selected

The lower part of the tab displays extra information for any single item selected in the previous table. If you select multiple downloads, only the details for the first item selected will be displayed.

The lower part of the tab has the following fields:

- **Current URL** - the current internet location.
- **Last Message** - the last message returned from the download location.
- **No of attempts** - the number of attempts to download the item.
- **Download state** - Downloading, Queued, etc.
- **Download speed** - the number of megabits per second (Mbps) at which the item is transferred.
- **Available URLs** - if there is more than one download location available, use this drop-down menu to select another internet location.

To manage downloads to the local Update Repository:

1. Select one or more downloads. This populates (some or all of) the details in the panel at the bottom of the page. If multiple items are selected, only the details for the item first selected is displayed.
2. Click one of the following buttons at the bottom of the panel:
   - Cancel Download (please see *Cancel Download* on page *94*) (applies to one or more downloads)
   - Pause download (please see *Pause Download* on page *94*) (applies to one or more downloads)
   - Resume download (please see *Resume Download* on page *95*) (applies to paused downloads only)
   - Open in browser (please see *Open in Browser* on page *95*) (applies to single selections only)

   When an update has finished downloading:
   - in the **Downloads** panel, the item is removed from the queue
   - in the **Updates** panel, the **Status** of the item changes to **Downloaded**.

Cancel Download

Some downloads in progress may no longer be required. You can always cancel these.

1. Select the download that you want to cancel.
2. Click the **Cancel download** button. The download is cancelled without any message. The number in the **Downloads (**n**)** tab is decremented (where n is the number of queued downloads).

Pause Download

During periods of high network usage, you may want to pause any active downloads.

1. Select the download that you want to pause.
2. Click the **Pause download** button. The download is paused without any message. The **Status** column now reports **Download paused**. The number in the **Downloads (**n**)** tab remains unchanged (where n is the number of queued downloads).

Resume Download

Downloads that were paused during busy network periods or at any other time, can always be restarted.

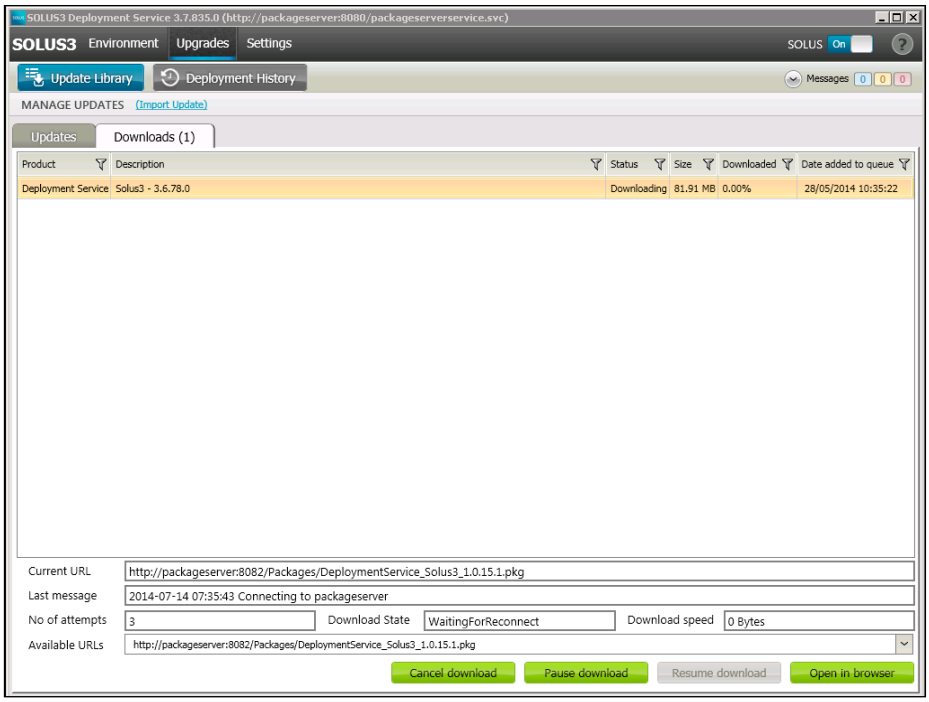
1. Select the download that you want to resume.
2. Click the **Resume download** button. The download resumes without any message. The **Status** column now reports **Download queued**. The number in the **Downloads (**n**)** tab remains unchanged (where n is the number of queued downloads).

Open in Browser

There may be occasions when SOLUS3 cannot download updates successfully. This can be caused by network issues at your LA, at your school, at Capita SIMS, or the Internet in general. You can download an update by using HTTP via your web browser. If you download an update via your web browser, the update must be imported into SOLUS3 manually.

To download updates:

1. Select **Upgrades | Update Library** to display the **MANAGE UPDATES** page with the **Updates** and the **Downloads** tabs.
2. Select the **Downloads** tab to display a list of updates in the queue.
3. Select the download that you want to open to populate the details in the panel at the bottom of the page.



4. Click the **Open in browser** button to display the message **Do you want to save this file, or find a program to open it?**
   - Click the **Find** button to open a web browser to search the web for a program which opens the selected file.
   - Click the **Save** button to open Windows Explorer and save the file.
   - Click the **Cancel** button to exit the **File Download** dialog.

5. Save the update file to your local computer.
6. After the update has completed downloading, import the update into SOLUS3.

   After downloading and importing the update manually, the **Status** in the **Updates** tab displays **Downloaded**. The update is now available for deployment.

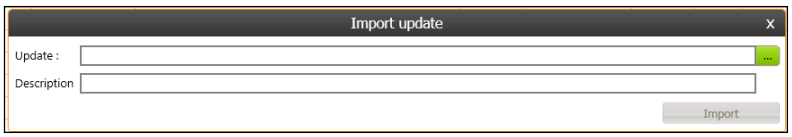
Import Update

If your site has limited bandwidth, you can import updates from Capita SIMS CDs. This enables large update files to be distributed to low-bandwidth sites, without burdening the network.

> ***IMPORTANT NOTE:*** *Because updates must be validated by Capita SIMS before they can be deployed, you still require an Internet connection to use SOLUS3. LAs and schools can only import updates for which they have been authorised.*

To import an update from CD:

1. Select **Upgrades | Update Library** to display the **MANAGE UPDATES** page.
2. Click the **Import Update** link to display the **Import update** dialog.



3. To locate the update file to import, click the green **Browse** button adjacent to the **Update** field.
4. In the **Open** dialog, navigate to the desired update file. The file must have the **.**pkg file extension.
5. Click the **Open** button to quit the dialog and populate the **Update** and **Description** fields.
6. To copy the update to the Update Repository, click the **Import** button.
7. When the import has finished, click the **Close** button.

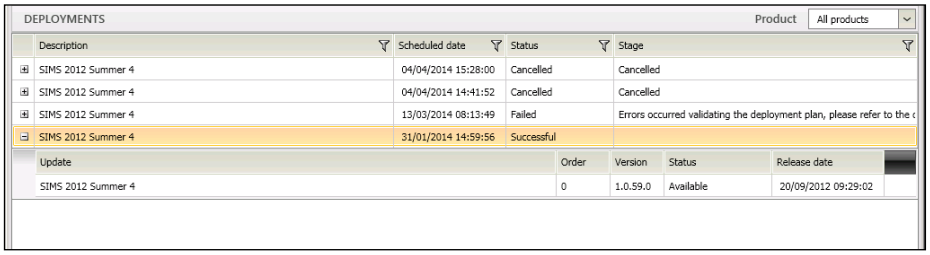
Deployment History

This panel contains all/any completed deployments.

Select **Upgrades | Deployment History** to display the **DEPLOYMENT HISTORY** page.

Viewing Deployments

To view dependencies for this update, click the plus button on the left-hand side. To collapse this information, click the minus button.



The **DEPLOYMENTS** panel displays the following columns:

- **Description** - a brief description of the deployment.
- **Scheduled Date** - the date that the required update is planned to take place.
- **Status** - e.g. **Cancelled**, **Successful**, etc.
- **Stage** - provides additional information on the reported status.

When you select an update from the list, one or more buttons become available on the right-hand bottom of the **TARGETS** panel:

- **Redeploy**
- **Cancel**
- **View log**
- **View detail**.

Viewing Deployment Targets

This panel contains status information for the following targets:

- SIMS File Server
- SIMS SQL Server
- SIMS Workstation

When you select an update from the list, one or more buttons become available on the right-hand bottom of the panel:

- **Redeploy**
- **Cancel**
- **View log**
- **View detail.**

The **TARGETS** panel displays the following columns:

- **Target name** - the name of the target to which the update was deployed, e.g. the **SIMS File Server**, the **SIMS SQL Server** and **SIMS workstation**.

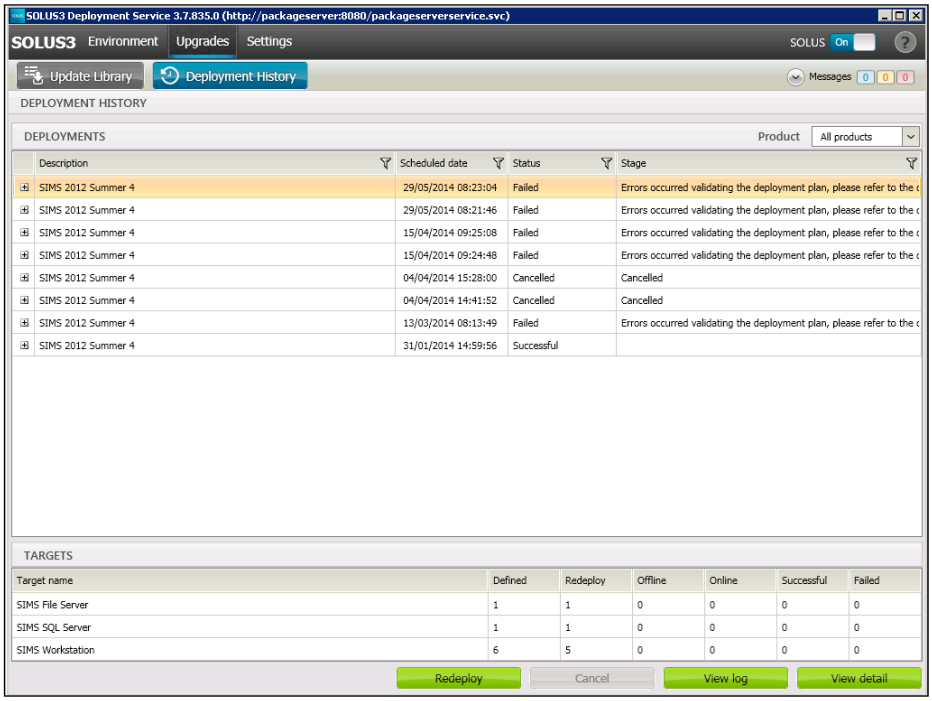
- **Defined** - the total number of targets of this type, defined in the DE for those sites that have been selected for this deployment.
- **Redeploy** - the total number of targets of this type, defined in the DE for those sites that have been selected for redeployment.
- **Offline** - the number of defined targets that were offline at the time of this deployment.
- **Online** - the number of defined targets that were online at the time of this deployment.
- **Successful** - the number of defined targets to which the update was successfully deployed.
- **Failed** - the number of defined targets to which updates were not successfully deployed.

Click the **View Detail** button for more information.

Redeploying a Deployment

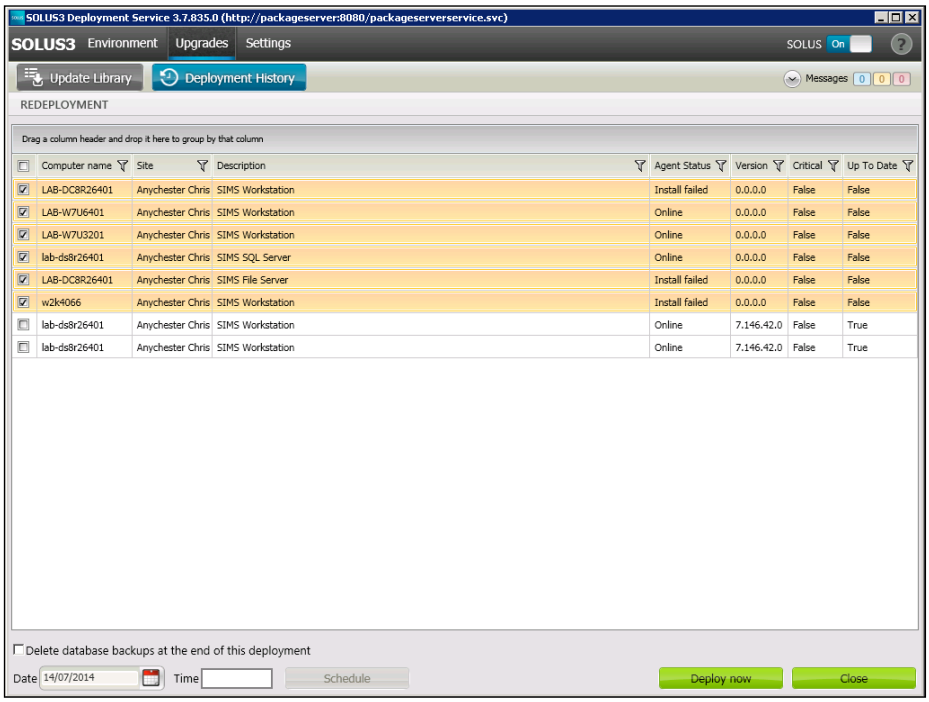
1. In the **DEPLOYMENTS** panel, select one or more deployments.

   To view dependencies for this update, click the plus button on the left-hand side. To collapse this information, click the minus button.



2. In the **TARGETS** panel, click the **Redeploy** button to display the **REDEPLOYMENT** panel.

Computers that do not require updating are not selected.



The **DEPLOYMENTS** panel displays the following columns:

- **Computer name** - target computer name
- **Site** - target site
- **Description** - target description
- **Agent status** - e.g. **Offline**, **Install failed**, etc.
- **Version** - software version
- **Critical** - **True** or **False**
- **Up to Date** - **True** or **False**

1. Select one or more computers. Optionally, select the **Delete database backups at the end of this deployment** check box.

   This means you will not be able to roll back your installation, should there be any issues with the deployment.

2. You can redeploy in two ways:

   - Immediately
     a. Click the **Deploy now** button.
     b. Click the **Yes** button to confirm the **Deploy now** dialog.
     c. Click the **OK** button to confirm the **Deployment plan rescheduled** dialog.
   - Scheduled
     a. Select the deployment **Date**.

        You can skip this field if you are setting a time for today.

     b. Enter the deployment **Time** in a 24-hour format.

        The **Time** set has to be at least 10 minutes from now.

c. Click the **Schedule** button.

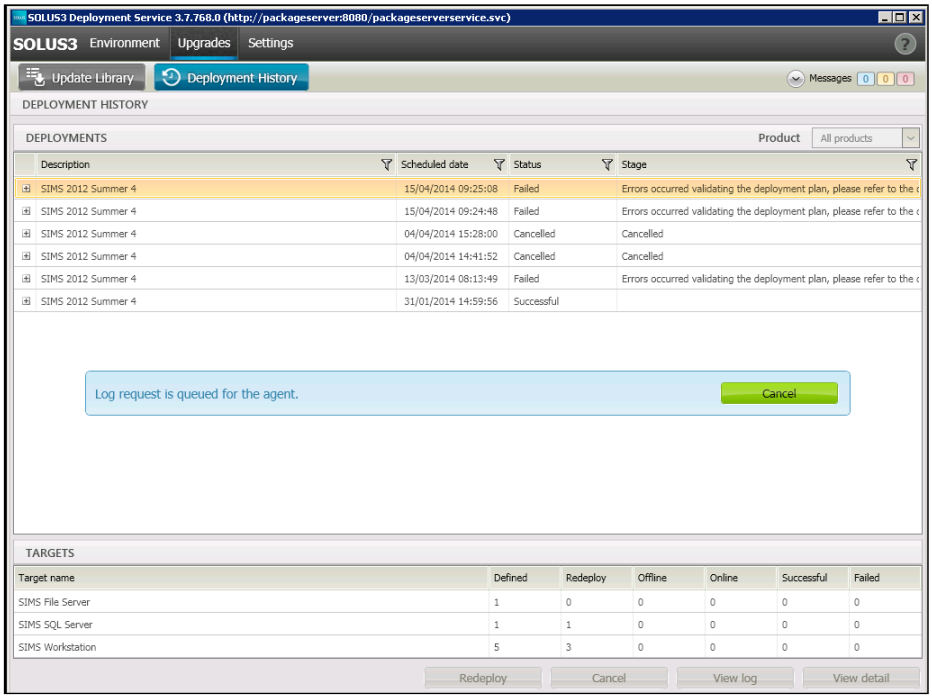
3. Click the **Close** button.

Cancelling a Deployment

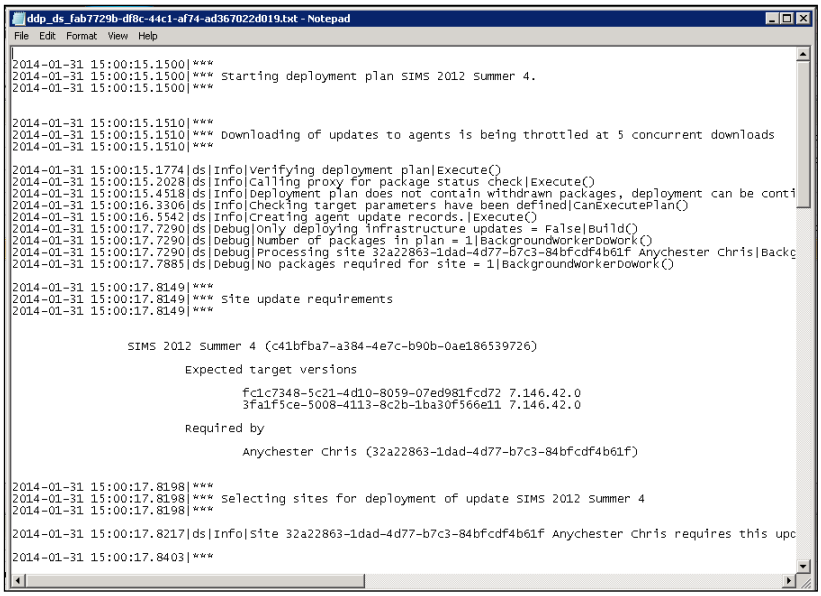
1. Select one or more deployments from the **DEPLOYMENTS** panel and then click the **Cancel** button.
2. Click the **Yes** button to confirm the cancellation.

Viewing Deployment Logs

1. Select one or more deployments from the **DEPLOYMENTS** panel.
2. Click the **View log** button to request a log for the agent.
3. SOLUS displays the message **Log request is queued for the agent**. Click the **Cancel** button to withdraw the request.



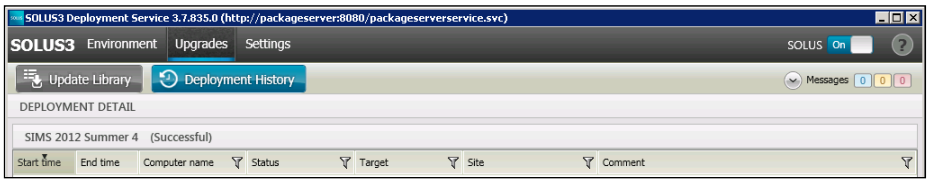
SOLUS3 displays the message **Log request is queued for the agent** and opens the required log on-screen in Notepad.



1. Save or print, as required.
2. Exit Notepad.

Viewing Deployment Details

1. Select a deployment from the **DEPLOYMENTS** panel and then click the **View detail** button to display the **DEPLOYMENT DETAIL** page.



The **DEPLOYMENT DETAIL** panel displays the following columns:

- **Start time**
- **End time**
- **Computer name**
- **Status**
- **Target**
- **Site**
- **Comment**

2. Click the **Agent deployment log** button for more details.
3. Click the **Back** button.

Working with Backups

> ***IMPORTANT NOTE**: Although SOLUS makes backups of the databases to which it deploys updates, this is not a substitute for a regular and comprehensive database backup plan.*

When SOLUS3 deploys an update, the default behaviour is to create backups of all affected databases.

If you select the **Delete database backups at the end of this deployment** check box at the bottom of the **Update deployment** or **Deployment history** pages, the default action for a deployment will be to delete the database backups made by SOLUS3. This can be changed on a per-deployment basis when scheduling the deployment.

Locating Backups

When SOLUS3 deploys an update that includes a database change, it creates a backup that can be restored in case of failure.

Default backup location:

`C:\Program Files\Microsoft SQL Server\MSSQL10_50.<InstanceID>\MSSQL\Backup`

Naming Convention

Each database backup is named according to the following convention:

`<Database name> <(Instance name)> <Date and Time>.bak`

Example: `SIMS (SqlExpress) 20111201T032415.bak`

The date and time are displayed in the format: `YYYYMMDDTHHMMSS`

Deleting Backups Manually

When a database backup is no longer needed, it can be deleted. The default location for these backups is the Microsoft SQL Server backup folder, e.g. `C:\Program Files\Microsoft SQL Server\MSSQL10_50.n\MSSQL\Backup` (where `n` is the number of the server instance).

If you want to delete a database backup immediately after a successful update, the default location of the backup is `C:\Windows\Temp`.

Installing SIMS on a New Device

SOLUS3 can install SIMS workstation software on new devices that have not previously had the software installed. To enable SOLUS3 to install SIMS workstation software, you must assign the new device the SIMS workstation target type. After assigning the device the SIMS workstation target type, SOLUS3 pushes the SIMS workstation software to the new device.

Installing FMS on a New Device

SOLUS3 can install FMS workstation software on new devices that have not yet had the software installed previously. To enable SOLUS3 to install FMS workstation software, you must assign the new device the FMS workstation target type. After assigning the device the FMS workstation target type, SOLUS3 pushes the FMS workstation software to the new device.

10 | Running an Upgrade

Deploying Updates for Schools - Checklist

Complete	Description
☐	Check for new updates.
☐	Download the required updates to your Update Repository.
☐	Deploy the updates.

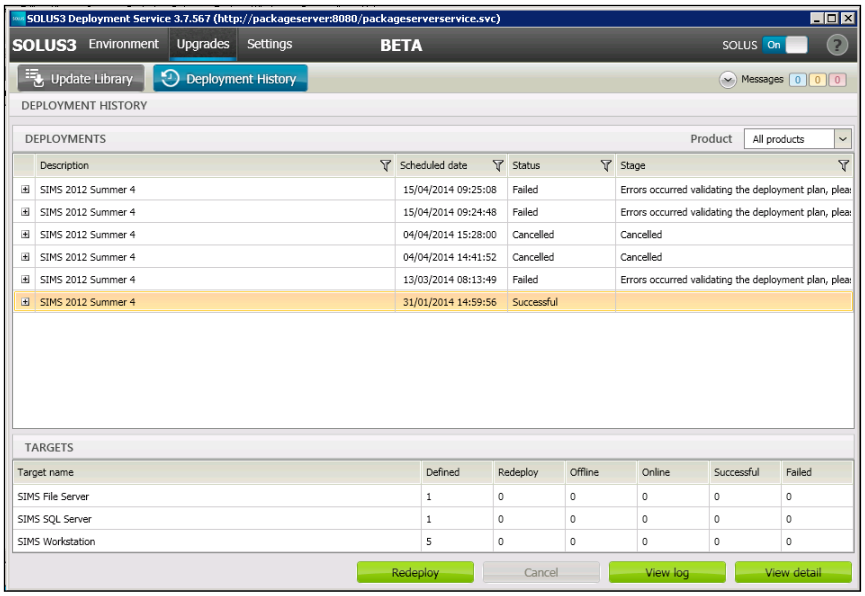
Deploying Updates

After your Local Authority, or Capita SIMS has authorised an update to a school's DS, you can deploy the update in the school to all devices with the correct target type.

Introduction to Managing Deployments

NOTE: This chapter covers tasks that can only be completed after a deployment plan has been created. The Managing Updates chapter details the process of creating a deployment plan.

Important information about deployments is presented to the Deployment Manager on the **Deployment History** page. Deployment Managers can see which deployments are scheduled and which are completed, as well as the updates and target types affected by the deployment. The Deployment Manager can also cancel and reschedule deployments, view the details of currently running deployments, and view the details of completed deployments.



Details in the **Targets in the deployment** panel apply only to that specific deployment attempt. This is illustrated in the following example.

There is an update that intends to upgrade SQL server target types and the SIMS database target types. On the first deployment attempt, if the SQL server targets were updated successfully, but SIMS database targets were not, then the **Successful** and **Failed** numbers in the **TARGETS** panel would reflect this. On the second deployment attempt, SOLUS3 would recognise that the SQL server targets had previously been updated and only upgrade the SIMS database targets. Although both targets are now successfully upgraded, the **TARGETS** panel for the second attempt would show that only the SIMS database target types completed successfully.

SOLUS3 and Wake-on-LAN

The SOLUS3 DS supports Wake-on-LAN (WOL).

Wake-on-LAN (WOL) technology enables you to access devices remotely as long as they have:

- a network connection
- a connection to a power source.

Devices do not have to be switched on; so-called "flea power" provides enough energy to allow the network interface to remain active and control access to full mains power. In doing so, WOL provides always-on access to remote devices while keeping power consumption to an absolute minimum.

When SOLUS3 begins a deployment, it sends a Wake-on-LAN packet to all the devices in the DE, and then waits 10 minutes before deploying any updates. Any devices in your DE with Wake-on-LAN enabled should then be ready for the deployment.

Capita Service Desk Support for WOL

WOL is third party technology and greatly dependent on your network, hardware, and software configuration. As a result the Capita Service Desk can support WOL only on a best-effort basis. Given the numerous configurations, it is impossible to recreate scenarios to resolve underlying networking issues. However, the troubleshooting steps should help to ensure that the necessary hardware and software configuration requirements are met.

Wake-on-LAN - Hardware Requirements

IMPORTANT NOTE: *If any of the following is in doubt, check with your hardware supplier.*

To use WOL, your workstations must have:

- a power supply that meets ATX (Advanced Technology eXtended) 2.01 or later specifications.
- a motherboard with an embedded Ethernet controller that supports WOL

  or
- a motherboard that uses a plug-in Network Interface Controller (NIC)

  Motherboards using a plug-in Network Interface Controller (NIC) may need an extra 3-pin cable connecting the NIC to the motherboard. Consult your hardware vendor if in doubt.

  Also see the Intel WOL information website (http://www.intel.com/support/network/adapter/pro100/sb/cs-008438.htm).

Wake-on-LAN Troubleshooting

DISCLAIMER: *The following instructions apply to third party technologies. These include, but may not be limited to, Network Interfaces using Wake-on-LAN (WOL) technology, Anti-Virus (AV) solutions, hardware based firewalls, and software based firewalls. As a result, Capita SIMS provides these instructions on a best-effort basis only. While Capita SIMS has made every attempt to be as complete and correct as possible, we cannot guarantee or verify this, and we are not responsible for any consequences resulting from the use of these instructions in any way, shape, or form. Also note that any changes and updates to these procedures referred to may not be reflected in these instructions.*

For the purpose of the following instructions, Capita SIMS does not support, configure or maintain customer networks, and we are not responsible for anything you may choose to do after following these instructions. Capita SIMS highly recommends that changes to your network environment be carried out by certified IT professionals. Capita SIMS further advises to consult your hardware vendor if you experience issues with your network interfaces.

After every check, verify if the issue is resolved.

- Ensure your computers meet the requirements described.
- If you have a motherboard based Network Interface Controller (NIC).
  - Ensure the Wake-on-LAN option is enabled in the Advanced BIOS options of your computer.

    Refer to your computer documentation on how to enter the BIOS setup mode on start-up.
  - Verify the Wake-on-LAN option is enabled in the Windows Device Manager of your computer.

    Refer to your operating system documentation on how to access the properties for your NIC using the Device Manager.
- If you have a plug-in Network Interface Controller (NIC)
  - Ensure the Wake-on-LAN option is enabled in the firmware of your NIC.

    Refer to your operating system documentation on how to access the properties for your NIC using the Device Manager.

    The WOL options are generally located under the Advanced, or the Power Management tab.
  - Verify the appropriate 3-pin cable connects your plug-in NIC with your motherboard.
- Ensure your computers are in the same domain.
- To exclude your Anti-Virus (AV) solution causing the issue, verify the AV detection logs.

  If your AV solution causes the issue, add ports **52966** and **52965** as exceptions. Consult your AV documentation for instructions.

  The WOL (Magic) Package is transmitted over UDP port 7 on the standard IP broadcast address (255.255.255.255).

- To exclude your firewall causing the issue, turn the firewalls off locally and on the Solus3 server.

  If this resolves the issue, add ports **52966** and **52965** as exceptions. Consult your firewall documentation for instructions.

  The WOL (Magic) Package is transmitted over UDP port 7 on the standard IP broadcast address (255.255.255.255).
- On one of the local computers:
  a. Locate the folder `c:\ProgramData\Microsoft\Crypto\RSA` (hidden by default as a system folder in Windows 7).
  b. Right-click the `MachineKeys` folder, and then select **Properties** from the pop-up menu to display the **MachineKeys Properties** page.
  c. Select the **Security** tab, and then click the **Advanced** button to display the **Advanced Security Setting for MachineKeys** page.
  d. Select the **Owner** tab to verify the **Current owner** is **Administrator**.
  e. Click the **OK** button to return to the **MachineKeys Properties** page.
  f. On the **Security** tab, click the **Edit** button to display the **Permissions for MachineKeys** page.
  g. Select **Everyone**, and then click the **Allow** check box for **Full control**.
  h. Click the **OK** button to return to the **MachineKeys Properties** page.
  i. Click the **OK** button to exit the **MachineKeys Properties** page.

  If this resolves your issue, apply the solution to all computers affected.
- In the folder `C:\Program Files`, verify you have a folder called `Solus3`. If this is missing, create one manually. Try the Agent installer again from the Solus3 server UI .
- Verify the Agent configuration:
  a. In the folder `C:\Program Files\Solus3\Agent service`, open the file `Sims.Solus3.Agent.AgentService.exe.config` using Notepad.
  b. Verify the ports are listed are **52966** and **52965**.
  c. If you need to correct them, run `services.msc` and then restart Solus3 Agent Services.
- Down-Level Logon Name:

  When you send the Agent from the Solus3 Server, you are asked to supply a user name (and password). Ensure you use the Down-Level Logon Name format: <DomainName>\Administrator

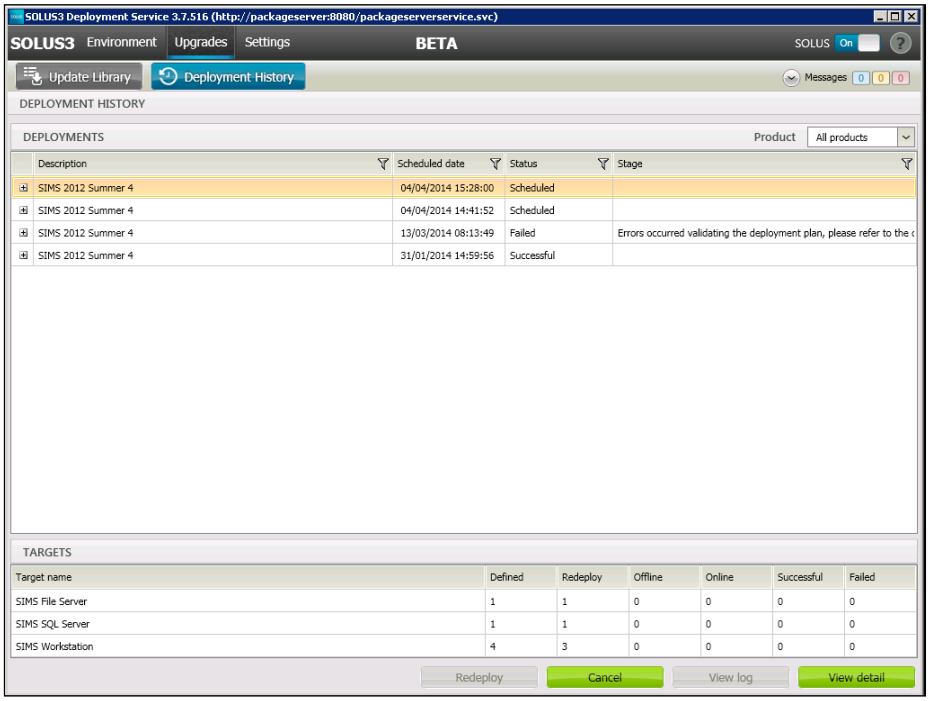
  Where <DomainName> is the name of your domain. Do not use the user name only.

Additional information is available (http://msdn.microsoft.com/en-us/library/windows/desktop/aa380525(v=vs.85).aspx).

Cancelling a Deployment

Deployment Managers can cancel a scheduled deployment.

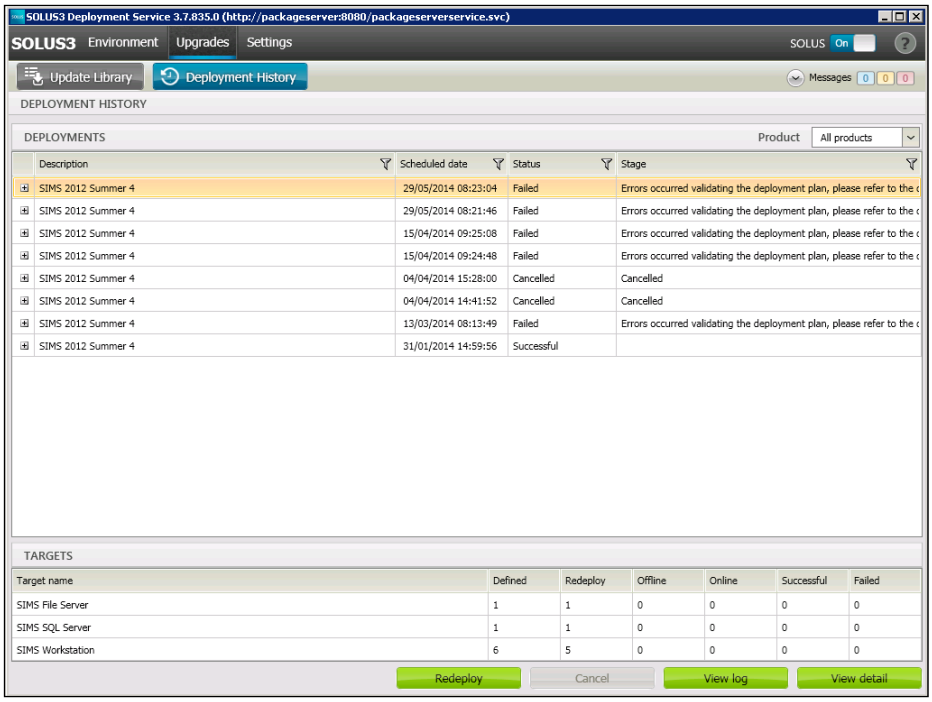
1. Select **Upgrades | Deployment History** to display the **Deployment history** pane, which contains a list of deployments (please see *Introduction to Managing Deployments* on page *105*).
2. Select one or more deployments that you want to cancel.
   - To select multiple consecutive items in a table, use **Shift + click**.
   - To select multiple, non-consecutive devices in a table, use **Ctrl + click**.



3. Click the **Cancel** button to display the **Cancel deployment plan?** dialog.
4. Click the **Yes** button to confirm the cancellation.

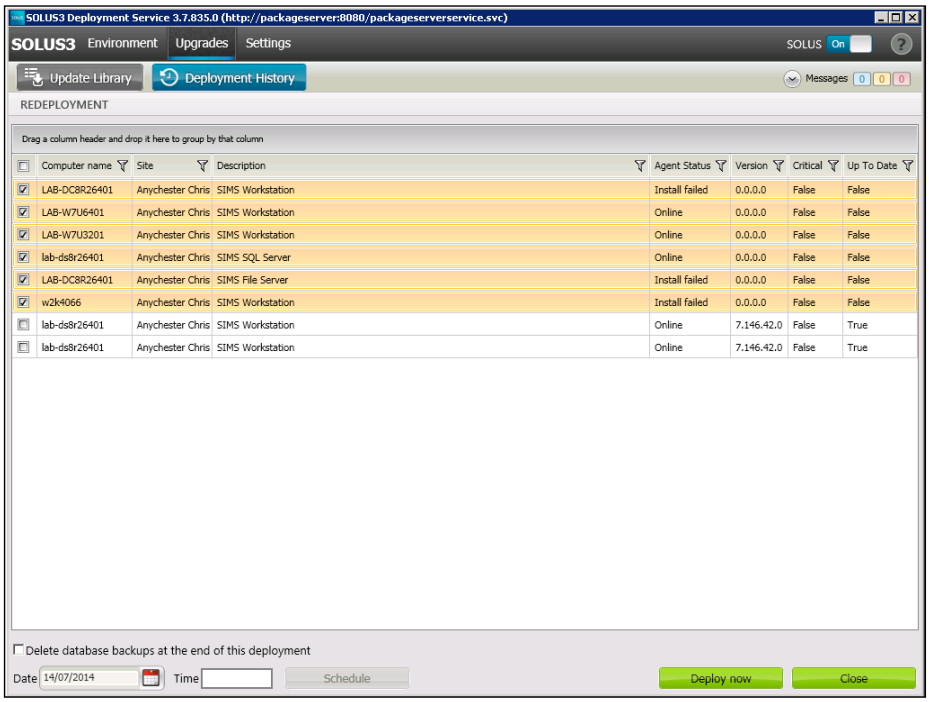
Rescheduling a Deployment

1. From the **DEPLOYMENTS** panel, select one or more deployments. To view dependencies for this update, click the plus button on the left-hand side. To collapse this information, click the minus button.



2. Click the **Redeploy** button to display the following columns:
   - **Computer name**
   - **Site**
   - **Description**
   - **Agent Status** - e.g. **Offline**, **Install failed**, etc.
   - **Version**
   - **Critical** - True or False.
   - **Up to Date** - True or False.

Computers that do not need to be updated are not selected.



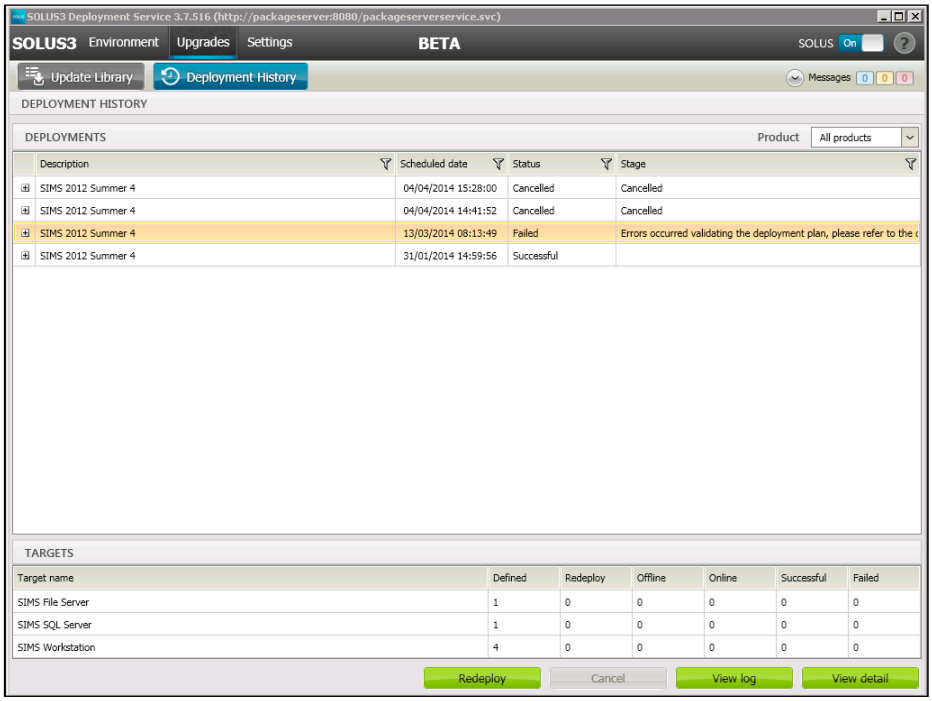
3. Select one or more computers. Optionally, select the **Delete database backups at the end of this deployment** check box. Selecting this option will result in you not being able to roll back your installation, should there be any issues with the deployment.
4. The following options are available:
   - Deploy immediately:
     a. Click the **Deploy now** button.
     b. Click the **Yes** button to confirm the **Deploy now** dialog.
     c. Click the **OK** button to confirm the **Deployment plan rescheduled** dialog.
   - Deploy in the future:
     a. Select the deployment **Date**.
     You can skip the **Date** field if you are setting a time for today.
     b. Enter the deployment **Time** in a 24-hour format.
     The **Time** set has to be minimally 10 minutes from now.
     c. Click the **Schedule** button.
5. Click the **Close** button.

Redeploying an Update

Sometimes it is necessary to redeploy a previously successful update to the same device. This may be required, for example, if SIMS program files were deleted from a device for troubleshooting purposes, or if the SIMS database was rolled back to a previous version and needs to be updated again.

However, after an update has been applied successfully to a specific device, the same update cannot be deployed again via the **Manage Updates** area. To deploy an update to a device that had previously been updated successfully, you must use the **Redeploy** button on the **DEPLOYMENT HISTORY** page.

1. Select **Upgrades | Deployment History** to display a list of previously scheduled deployments.

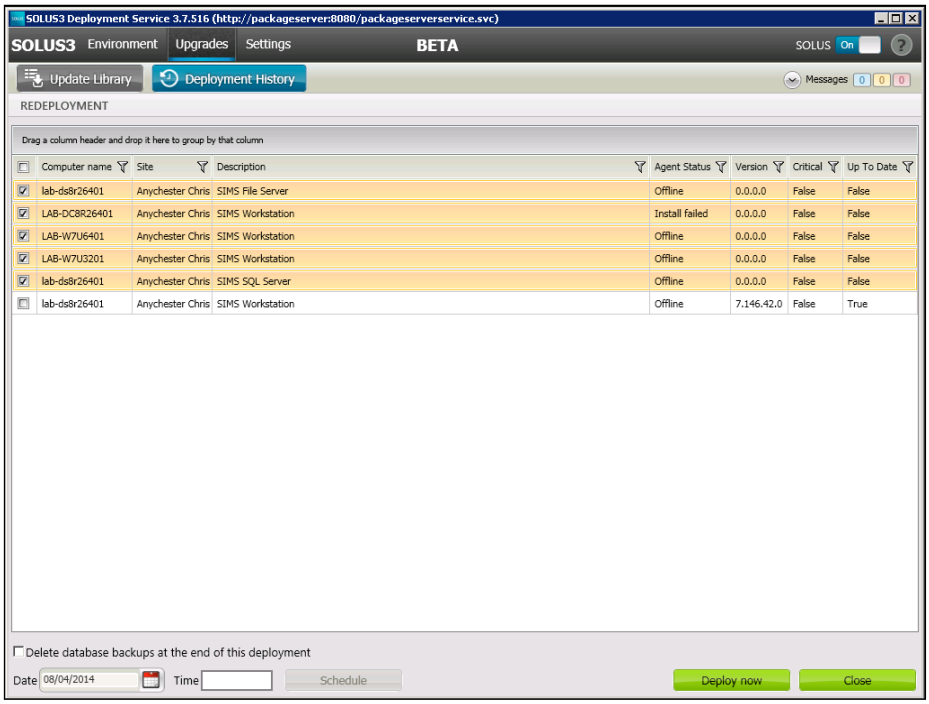


2. If necessary, use the filters in the navigation bar on the left to find the update that you wish to redeploy.

   To view dependencies for this update, click the plus button on the left-hand side. To collapse this information, click the minus button.

3. In the **DEPLOYMENT HISTORY** page, select the required deployment plan to display the deployment plan details in the **DEPLOYMENTS** and **TARGETS** panels.

4. In the **TARGETS** panel, click the **Redeploy** button to display a list of devices.



5. Select the check box for each device to which you wish to redeploy the update or use the buttons at the bottom of the page.
6. Click the **Save** button to return to the deployment details.
7. If you want to schedule the redeployment for a future date, enter a **Date** and **Time** in the fields at the bottom of the panel, then click the **Schedule** button.

   If you want to run the redeployment immediately, click the **Deploy now** button.

   After clicking either button, a confirmation dialog is displayed.
8. Click the **Yes** button to confirm the scheduled redeployment.
9. Click the **OK** button to complete the process.

Viewing and Storing a Deployment Log

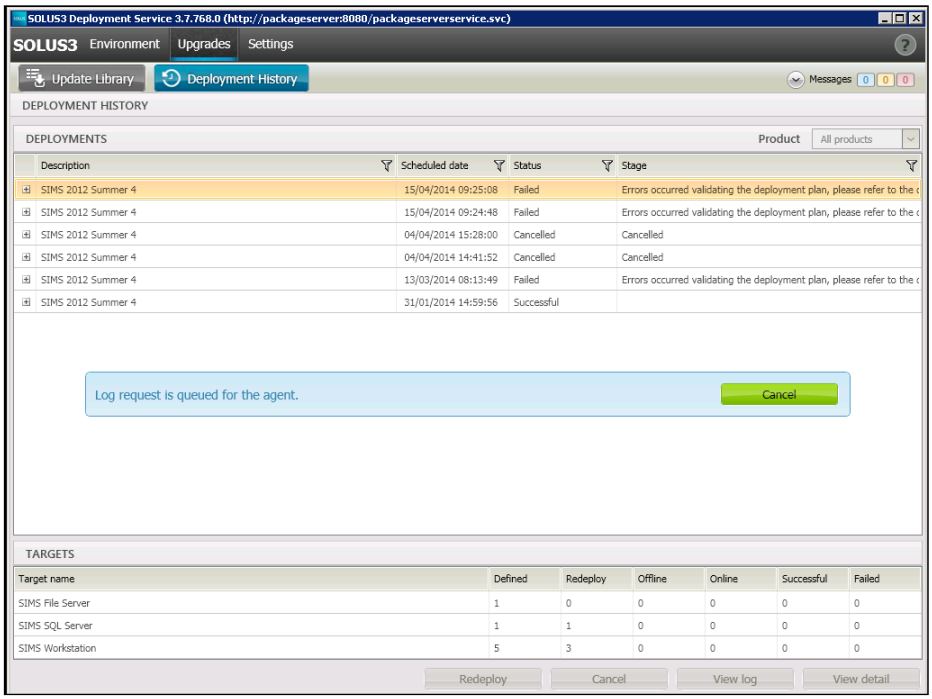
Deployment logs provide detailed information about each task that the Deployment Service attempted during the update process. Deployment logs can help when troubleshooting issues with deployments.

> ***IMPORTANT NOTE:*** *It is not possible to carry out any other tasks in SOLUS3 while your request is being processed. If required, click the* ***Cancel*** *button to retract the request.*

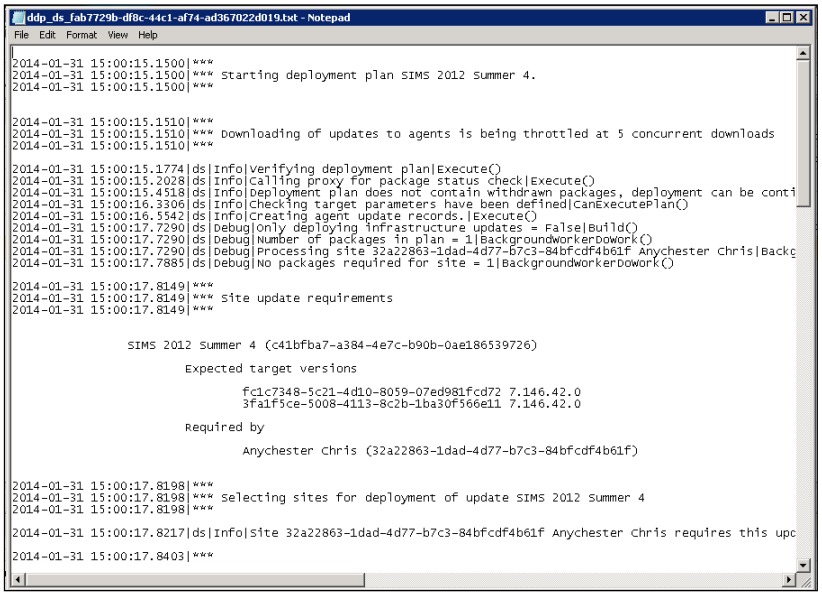
To view a deployment log for a specified deployment, complete the following procedure:

1. Select **Upgrades | Deployment History** to display a list of deployments.
2. Select the deployment for which you want to view the deployment log.

3. Click the **View log** button.



SOLUS3 displays the message **Log request is queued for the agent**. The required is displayed on-screen in Notepad.

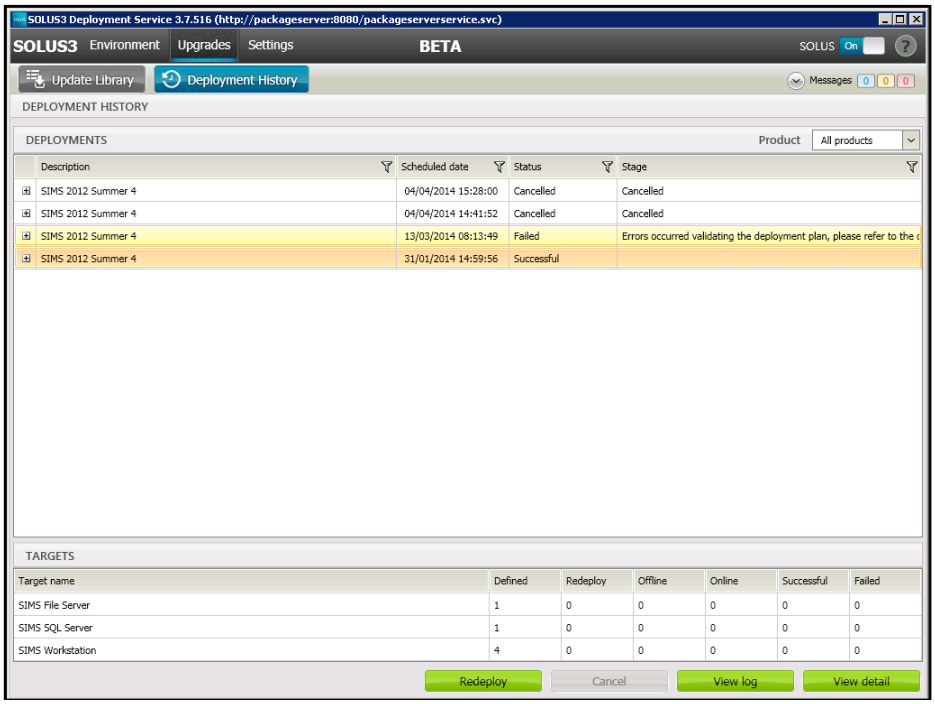


4. Save and print the file, if required.
5. Exit Notepad.

Viewing Deployment Details

Viewing the deployment details enables the Deployment Manager to determine the status of each package in a deployment on each device in the deployment.

1. Select **Upgrades | Deployment History** to display a list of deployments.



2. Select the deployment for which you want to display the details.
3. Click the **View Detail** button to display the **Deployment Detail** panel. This panel contains a list of each agent and target in the deployment.
4. Select the required deployment(s):
   - To select multiple consecutive items in a table, use **Shift + click**.
   - To select multiple, non-consecutive devices in a table, use **Ctrl + click**.
5. Click the **Agent deployment log** button.
6. Click the **Close** button to return to the **Deployment Detail** panel.
7. Click the **Back** button to return to the **Deployment History** page.

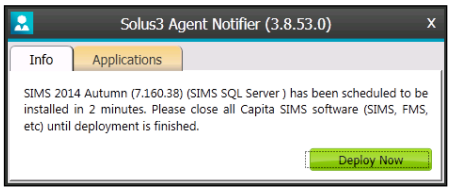
11 | Agent Notifier

Agent Notifier

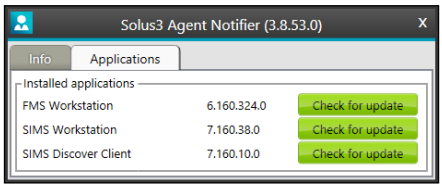
The Agent notifier is installed on each machine on which SOLUS3 is installed. Its purpose is to inform the user of any imminent SIMS upgrades.

To display the Agent Notifier, double-click the **SOLUS3 Agent Notifier** icon in the System Tray.

Agent Notifier icon



The **Info** tab informs the user of any imminent SIMS upgrades. Click the **Deploy Now** button, if required.



The **Applications** tab displays a list of **Installed applications**, together with their associated version numbers. This information is of particular importance to IT/support staff.

Clicking the **Check for update** button enables you to run upgrades manually from your machine, rather than wait for SOLUS to carry out an automatic deployment. Where more than one upgrade is available to your workstation, updates will be run in chronological order.

Clicking the **Check for update** button also sends the appropriate configuration files to the workstation that sent the request.

- Clicking this button for **SIMS Workstation** sends the `SIMS.ini` and `connect.ini` files to the workstation that requested it.
- Clicking this button for **FMS Workstation** sends the `fmsconnect.ini` file to the workstation that requested it.
- Clicking this button for **SIMS Discover Client**, the Discover configuration file is sent to the workstation that requested it.

Additionally, if an application becomes corrupt on your machine (and you are on the correct version), it is possible to re-install the current version on the machine.

12 | Viewing Reports

Introduction

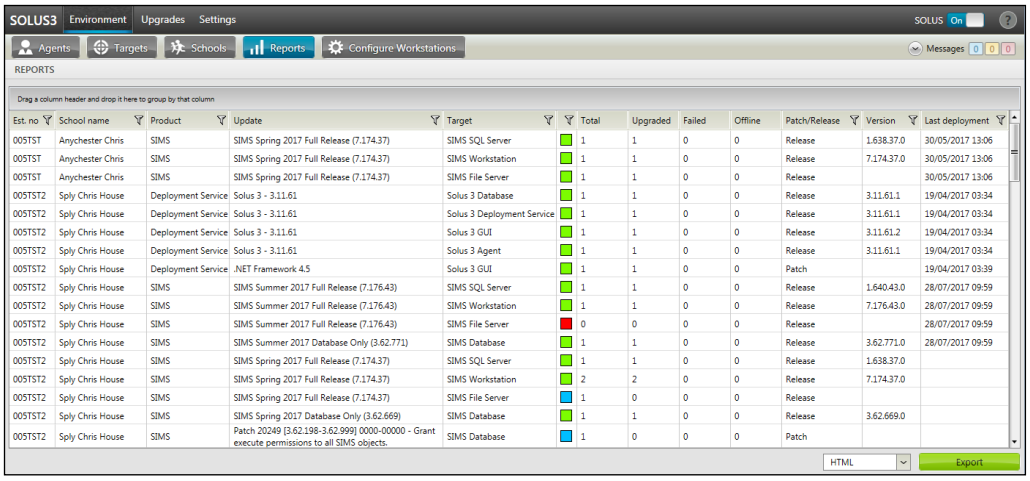
The SOLUS3 Reports function provides access to information about the DS (and child sites for LA's) and the deployment of updates. You can export reports to HTML, CSV and XLS format. This information can be used by Deployment Managers to verify that updates have been downloaded and deployed.

To change the way the output is presented, you can:

- change the column order.
- sort on any column.
- filter on all columns.
- group the output by column. This enables schools to focus on specific information. LAs and RCs might use this feature to display upgrade information by school.

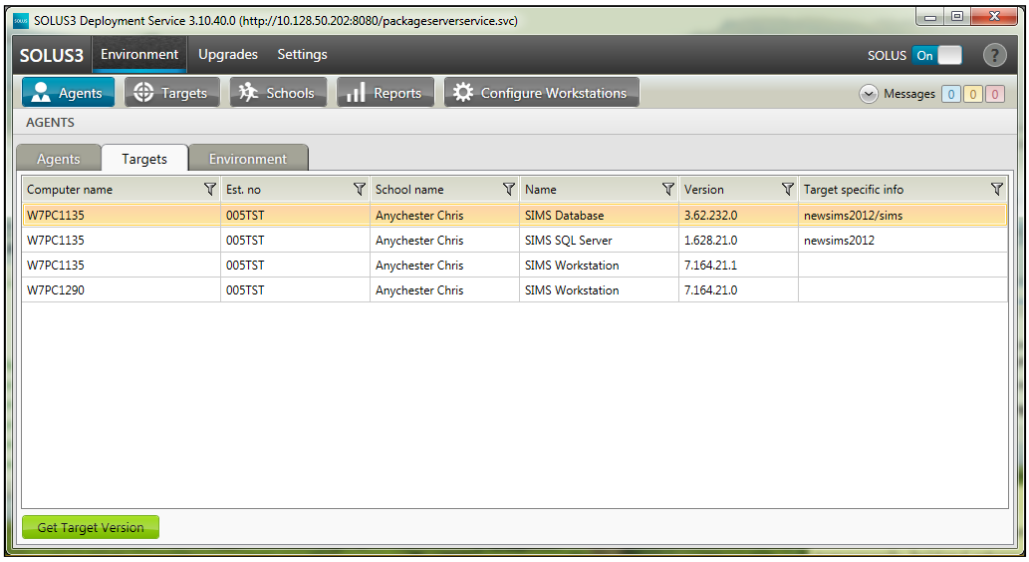
Viewing the Reports Page

Select **Environment | Reports** to display the **REPORTS** page.



The report displays the most up-to-date information (to within one hour - based on usual operating parameters of data exchange) on the last attempted upgrade for each target.

To view the version of software that a target (that has partially failed/failed its most recent upgrade) is currently using, select **Environment | Agents** and then select the **Targets** tab.



Running a Report

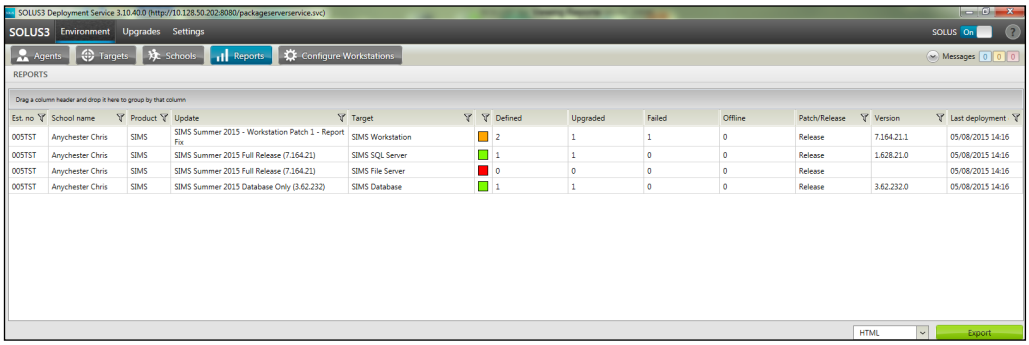
1. Select **Environment | Reports** to display the **REPORTS** page.

   The **REPORTS** page contains the report output for the selected school.

   The column names are:

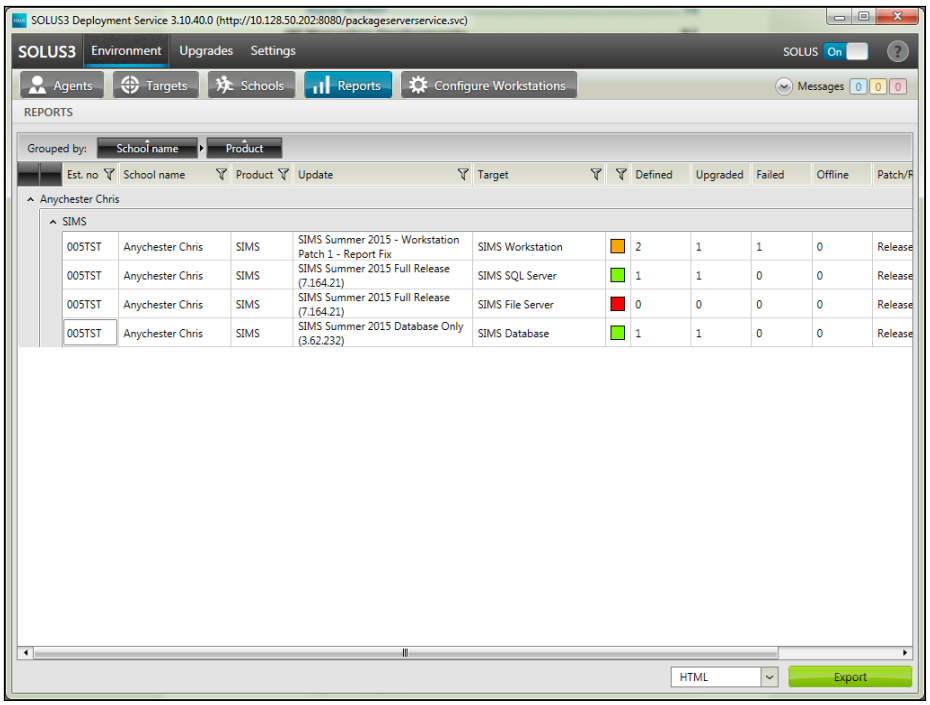
   - **Establishment number**
   - **School name**
   - **Product**
   - **Update** (last deployed update)
   - **Target**
   - Last update status (hover over to confirm status)
     - Green - Successful
     - Amber - Partially successful
     - Red - Failed
   - **Total** (number of targets identified for updating)
   - **Upgraded** (number of targets successfully updated)
   - **Failed** (number of targets failed)
   - **Offline** (number of targets offline)
   - **Patch / Release**
   - **Version**

- **Last deployment**



2. To re-order columns, click and drag the column headings as appropriate.
3. To sort a table on a particular column, click the column heading one or more times.
4. To filter a column, click the filter symbol for the relevant column, and then select from the drop-down menu or enter the required information.
5. To group the report, click and drag the appropriate column heading(s) onto the bar above the column headings.

   In the example below, we have used the columns **School name** and **Product**.



   To remove grouping criteria, close each of the column names (hover over them individually and click the cross button when it appears).

6. To sort on the selected groups, click the relevant column name(s) in the **Grouped by** field. Sorting grouped columns works in the same way as sorting columns.

   The **School names** group is sorted in alphabetical order.

7. To export the output:
   a. From the drop-down menu next to the **Export** button, select the output format:
      - HTML
      - CSV
      - XLS.
   b. Click the **Export** button.

      If you have not used the output format before, you may be asked which application you want to use to open the output file. Take care when making a selection because you will not be asked again. You can change the program that opens the file.
8. **Print**, **Save** or **Close** the output file.

13 | Deployment Checklist

Deploying Updates for Schools - Checklist

Complete	Description
❑	Check for new updates.
❑	Download the required updates to your Update Repository.
❑	Deploy the updates.

14 | Appendix

Sorting and Filtering Data Grids

Data grids are proprietary ASP.NET-based grids that enable administrators to use spreadsheet-like functionality to speedily load and handle large quantities of data. Data grids provide advanced sorting and filtering functionality, and have been made available for the migration of SQL target databases.

Data grids provide the following capabilities:

- Integrated paging, sorting, filtering and grouping functionality
- Scrolling with frozen columns and static headers
- Drag and drop rows to reorder or move to another grid
- Export to PDF and CSV file
- Export to Microsoft Word and Microsoft Excel format
- Multi-column headers and keyboard support
- Resizing rows
- Data-binding (server-side, client-side and web service)
- Hierarchy/NestedView template.

Using the Command Line

Setting up Schools via the Command Line

The Command Line UI feature enables users to streamline the initial configuration of SOLUS3, which is particularly useful when setting up multiple installations. This feature enables support teams that want to standardise installation to use repeatable steps.

> *NOTE: Before this functionality was introduced, entering school data required details to be entered for each school separately. You can still enter school details for each school separately, if required (please see* Registering a Site *on page* 26*).*

Details can be entered individually (using Command Line) or in bulk (using batch files).

Viewing Command Line Parameters for SOLUS3

The default command line exe can be found on the SOLUS3 UI in the following location:

```
C:\Program Files\DeploymentServerUI\Sims.Solus3.DeploymentServer.UI.CommandLine.exe
```

Running the command line exe with no values displays all of the commands on screen. The commands available are as follows.

Each command relates to a screen in the UI. Where the area has sub-settings, running the command line with no value returns further command options.

An example of the proxy command and sub settings is as follows:

```
C:\Program
Files\DeploymentServerUI\Sims.Solus3.DeploymentServer.UI.C
ommandLine.simsExtractUpdate -help
```

NOTE: Not all commands have sub-settings.

```
C:\Program Files\Solus3\DeploymentServerUI>Sims.Solus3.DeploymentServer.UI.Comma
ndLine simsExtractUpdate

C:\Program Files\Solus3\DeploymentServerUI>Sims.Solus3.DeploymentServer.UI.Comma
ndLine simsExtractUpdate -help
Sims.Solus3.UI 3.11.21.0
Copyright © Capita 2015

  -o, --extractAfterDownloadOn      Extract after download.

  -d, --extractAfterDeploymentOn    Extract after deployment.

  -u, --useSubFolderOn              Extract into a product sub folder.

  -f, --extractFolder               Path of MAIN folder to extract into.  Do
                                    not specify product sub folders.

  --help                            Display this help screen.
```

IMPORTANT NOTE: *Any item marked as* ***Required*** *must have a value submitted using the command line.*

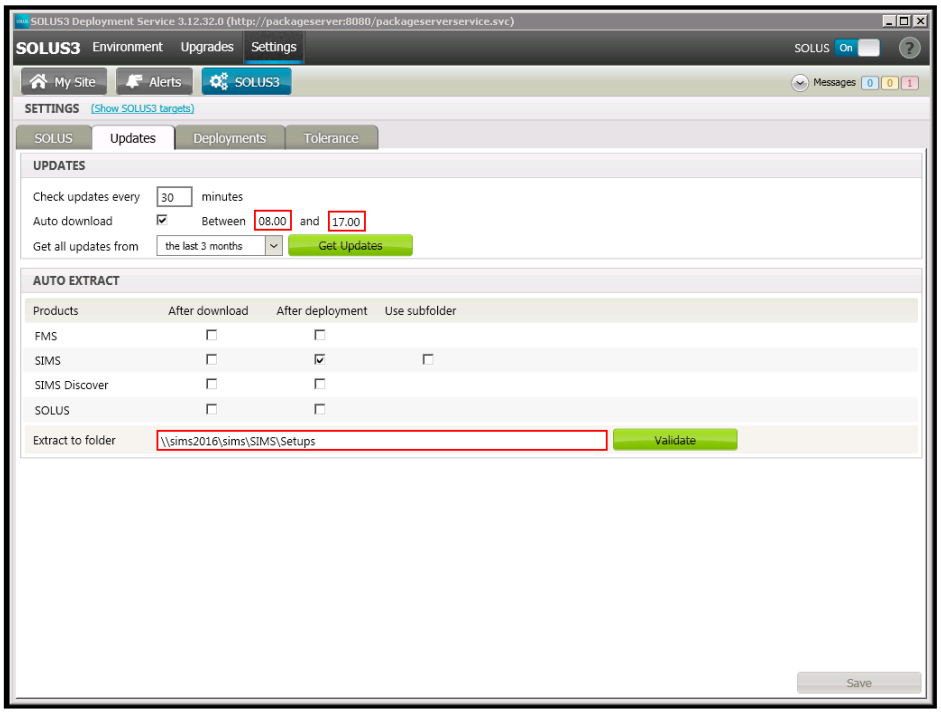
TIP: To run a command line, please refer to the UI for an example of the format required.

Example of a command line to set auto extraction after deployment:

```
C:\SOLUS3>"C:\Program Files\Solus3\DeploymentServerUI\Sims.Solus3.DeploymentServer.UI.CommandLine.exe" simsExtractUpdate
 --extractAfterDeploymentOn --extractFolder "\\sims2016\sims\SIMS\Setups"
C:\SOLUS3>
```

WARNING: *Commands are case sensitive. Enter them exactly as they are shown in the menu.*

The UI screen will reflect the values submitted via the command line.



NOTE: Further information regarding the implementation of the command line process is available as a downloadable hot topic on My Account.

Installing Multiple Schools via a Batch File

Using the command line, it is possible to create your own batch file that can be used when managing multiple installations.

To experiment with a batch file, you could use the following template.

***WARNING:** Please be aware that the following is an example only and is not supported by Capita.*

This makes the assumption that the computer running the batch file is the server running all of the SOLUS3, SIMS, FMS and Discover server components. It also assumes that the user running the batch file has permissions across the network to install any required SOLUS3 agent software. In this example, the SQL Instance is not named and the server is also running a SIMS, FMS and Discover client.

In the following example:

- Items that are specific to the school network (sometimes at more than one site) are displayed in blue text
- School-specific SOLUS UI values are displayed in red text.

1. Create a Notepad file with a suitable name.
2. Open the Notepad file and add the parameters one line at a time. A sample script for a school could look like the following.

```
set path="C:\Program Files\Solus3\DeploymentServerUI\Sims.Solus3.DeploymentServer.UI.CommandLine.exe"
set est=[dfe number]
set post="[postcode]"
set host=%COMPUTERNAME%
set servicemachine="LAB-DS8R26402"
set domainname=LAB-LA02\Administrator
set domainpass=[password]

@REM REGISTER
@REM %path% proxy --ProxyAddress xx.xxx.xxx.xx --ProxyDomainName xxx --ProxyPort 8080 --ProxyUsername Administrator --ProxyPassword %domainpass%
%path% register --estNumber %est% --postcode %post% --password "Password01"
%path% settings --repository "\\%host%\Repository" --service "%servicemachine%" --DomainUserName %domainname% --DomainPassword %domainpass%

%path% download --autoDownloadOn --autoDownloadStartTime 08:00 --autoDownloadEndTime 17:00 --autoDownloadAgentOn --autoDownloadAgentStart 08:00 --autoDownloadAgentEnd 17:00
@REM %path% download --AutoDownloadOff --autoDownloadAgentOff

@REM SCHEDULE
@REM %path% simsSchedule --autoDeploy --start 08:00 --end 17:00 --mon --tue --wed --thu --fri --sat --sun
@REM %path% fmsSchedule --autoDeploy --start 08:00 --end 17:00 --mon --tue --wed --thu --fri --sat --sun
@REM %path% discoverSchedule --autoDeploy --start 08:00 --end 17:00 --mon --tue --wed --thu --fri --sat --sun
@REM %path% solusSchedule --autoDeploy --start 08:00 --end 17:00 --mon --tue --wed --thu --fri --sat --sun

@REM SIMS TARGETS
%path% simsSql --serverAndInstance %host% --binn "C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\Binn" --estNumber %est% --DomainUserName %domainname% --DomainPassword %domainpass%
%path% simsDatabase --serverAndInstance %host% --databaseName sims1  --username sa --password Password01 --estNumber %est%  --DomainUserName %domainname% --DomainPassword %domainpass%
%path% simsDms --serverName %host% --installationPath C:\SIMS\DMS --estNumber %est% --DomainUserName %domainname% --DomainPassword %domainpass%
```

%path% simsFs --serverName %host% --installationPath "C:\SIMS\File Server" --estNumber %est% --DomainUserName %domainname% --DomainPassword %domainpass%

@REM FMS TARGETS

%path% fmsSql --serverAndInstance %host% --binn "C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\Binn" --estNumber %est% --DomainUserName %domainname% --DomainPassword %domainpass%

%path% fmsDatabase --serverAndInstance %host% --databaseName fms1 --username sa --password Password01 --estNumber %est% --DomainUserName %domainname% --DomainPassword %domainpass%

@REM DISCOVER TARGETS

%path% discoverDatabase --SimsServerAndInstance %host% --SimsDatabaseName sims1 --username sa --password Password01 --serverAndInstance %host% --databaseName Disco --estNumber %est% --DomainUserName %domainname% --DomainPassword %domainpass%

@REM %path% discoverDatabase --SimsServerAndInstance %host% --SimsDatabaseName sims1 --WindowsAuthentication Password01 --serverAndInstance %host% --databaseName Disco --estNumber %est% --DomainUserName %domainname% --DomainPassword %domainpass%

%path% discoverService --taskStartTime 08:00 --serverName %host% --installationPath C:\Discover --estNumber %est% --DomainUserName %domainname% --DomainPassword %domainpass%

@REM CLIENT TARGETS

%path% clients --discover --sims --fms --ComputerName %host% --estNumber %est% --DomainUserName %domainname% --DomainPassword %domainpass%

%path% clients --discover --sims --fms --ComputerName LAB-W7U3201 --estNumber %est% --DomainUserName %domainname% --DomainPassword %domainpass%

%path% clients --discover --sims --fms --ComputerName LAB-W7U6401 --estNumber %est% --DomainUserName %domainname% --DomainPassword %domainpass%

%path% clients --discover --sims --fms --ComputerName LAB-W7U3202 --estNumber %est% --DomainUserName %domainname% --DomainPassword %domainpass%

%path% clients --discover --sims --fms --ComputerName LAB-W7U6402 --estNumber %est% --DomainUserName %domainname% --DomainPassword %domainpass%

@REM CONFIGURE

```
%path% configure  --sims "C:\Solus3_Stuff\ini files\School1\sims.ini" --
sendSimsIni  --connect "C:\Solus3_Stuff\ini files\School1\connect.ini"  --
sendConnect  --fmsConnect "C:\Solus3_Stuff\ini
files\School1\FMSConnect.ini" --sendFmsConnect --sendDiscoverConfig  --
estNumber %est%


@REM ALERTS
%path% alerts  --ServerName "LAB-DS8R26402"  --PortNumber 25  --
UserName %domainname%  --Password %domainpass% --SenderEmail
alerts@solus.com  --UpdateEmail %updateemail%  --UpdateContent
%updatecontent%  --DdpEmail %ddpemail%  --DdpContent
%ddpcontent%


@REM SOLUS ON/OFF
%path% enable --solusOn
@REM %path% enable --solusOff


PAUSE
```

3. Rename the extension of the text file to `.bat`, e.g. `solus_command.bat`.
4. The batch file can be executed by double-clicking it in the document library. This adds all of the parameters into the SOLUS3 database at once.
5. The batch file can be edited and run again for each school.

Target Types – Required Additional Information

Some target types require that additional information is entered for SOLUS3 to properly update the Capita SIMS software. The following tables summarise the additional information required.

SIMS

Target Type	Required Information	Description
SIMS Workstation	Installation path	If the site does not use the default SIMS installation location, enter the location used by the site.
SIMS SQL Server	Instance name	The instance name of the SIMS SQL database.
	`binn` Folder Location	The `binn` folder location on the SIMS SQL server.
SIMS Database	Database name	The name of the SIMS database.

Target Type	Required Information	Description
	User name	The user name of a user with System Administrator access to the SIMS SQL database, usually the SA. Using a Windows Authentication user name will not work.
	Password/Confirm Password	The password of the user with System Administrator access to the SIMS SQL database.
SIMS DMS	Installation location	The installation location of the SIMS Document Management Server. The default location is `C:\Program Files\SIMS\ SIMS.net Document Server`.
SIMS File Server	Installation location	Local path to the location that stores SIMS documents.

Discover

Target Type	Required Information	Description
Discover Database	**IMPORTANT NOTE**: *To install the Discover database on a different SQL server and instance than the related SIMS database, you must use trusted Windows accounts to log into SIMS and perform several tasks after installing Discover. For more information, please refer to the* Discover Technical Guide, *available from the My Account website (*https://myaccount.capita-cs.co.uk*).*	
	Computer name	Computer name of the SQL server that will host the Discover database, e.g. `MYSERVER`.
	Instance name	The instance name of the Discover SQL database, e.g. `SIMS2012`.
	Database name	The database name of the Discover SQL database, e.g. `Discover`.
	User name	The user name that is used to log into the Discover database (only required if not using Windows Authentication). This user must have SA rights for the SQL server that is hosting the Discover database.
	Password	Password of the user name that is used to log into the Discover database (only required if not using Windows Authentication).

Target Type	Required Information	Description
	Confirm password	Re-enter the password used to log into the Discover database (only required if not using Windows Authentication).
	SQL Server name	Computer name of the SQL server hosting the SIMS database to which Discover relates.
	Instance name	The instance name of the SIMS SQL database to which Discover relates.
	Database name	The database name of the SIMS SQL database to which Discover relates.
Discover Windows services	Computer name	Name of the computer that will host the SIMS Discover Windows services.
	Installation path	Define the location of the SIMS Discover Windows services. If left blank, the services are installed to `C:\Program Files\SIMS\Discover` (32-bit Windows) or `C:\Program Files (x86)\SIMS\Discover` (64-bit Windows), where `C:\` is the local drive on which the services are to be installed.
	IMPORTANT NOTE: *Although Discover can be run using built-in Windows accounts, Capita SIMS recommends creating two new Windows user accounts for the Discover Data Transfer service and the Discover Group Synchronisation service.*	
	Use built-in account	Select a built-in account to run the Discover Data Transfer service.
	Use windows account	Select this option to define a different Windows account to run the Discover Data Transfer service.
	Domain\User name	The domain and user name of the account you wish to use to run the Discover Data Transfer service.
	Password	Password of the account you wish to use to run the Discover Data Transfer service.
	Confirm password	Re-enter the password of the account you wish to use to run the Discover Data Transfer service.

Target Type	Required Information	Description
	Use built-in account	Select a built-in account to run the Discover Group Synchronisation service.
	Use windows account	Select this option to define a different Windows account to run the Discover Group Synchronisation service.
	Domain\User name	The domain and user name of the account you wish to use to run the Discover Group Synchronisation service.
	Password	Password of the account you wish to use to run the Discover Group Synchronisation service.
	Confirm password	Re-enter the password of the account you wish to use to run the Discover Group Synchronisation service.
	Start time	Time to start the scheduled tasks for Discover.
	SQL Server name	Name of the SQL server hosting the Discover database related to these services.
	Instance name	The instance name of the Discover SQL database related to these services.
	Database name	The database name of the Discover SQL database related to these services.
Discover Client	*NOTE: You will need to select each device on which you wish to install the Discover client in the area marked '1' of the Discover client configuration page.*	
	Installation path	The location you wish to install the Discover client. Leave blank to use the default installation path, `C:\Program Files\SIMS\Discover Client`, where `C:\` is the local drive on which the Discover client is to be installed. If you require a different installation path, enter it here.

Target Type	Required Information	Description
	SQL Server name	Computer name of the SQL server hosting the Discover database related to these clients.
	Instance name	The SQL instance name of the Discover SQL database related to these clients.
	Database name	The database name of the Discover SQL database related to these services.
	Use this website	The address of the Discover website from which the client accesses Discover data.

FMS

Target Type	Required Information	Description
FMS Workstation	Installation path	If the site does not use the default FMS installation location, enter the location used by the site.
FMS SQL Server	Instance name	The instance name of the FMS SQL database.
	`binn` Folder Location	Location of the `binn` folder on the FMS SQL server.
FMS Database	Database name	The name of the FMS database.
	User name	The user name of a user with System Administrator access to the FMS SQL database, usually the SA (using a Windows Authentication user name will not work).
	Password/Confirm Password	The password of the user with System Administrator access to the FMS SQL database.

IMPORTANT NOTE: *If your FMS configuration includes both an FMS database and an FDS database, you should configure two FMS Database targets, one for each database.*

SIMS and Discover Database Permission Requirements

When you define database targets for SIMS and Discover, you must enter a user name and password. Generally, the SA user name and password should be used. However, there may be situations where the database administrator wants to create a new user account just for enabling SOLUS3 to upgrade and restore databases.

Any user account that SOLUS3 uses to upgrade a SIMS or Discover database must have the following SQL Server roles and role memberships assigned.

Required Server Roles	Required Role Memberships (for the SIMS or Discover database)
dbcreator securityadmin	db_owner db_backup_operator

FMS Database Permission Requirements

When defining database targets for FMS, you must enter a user name and password. Generally, you should use the SA user name and password. However, there may be situations where the database administrator prefers to create a new user account exclusively for enabling SOLUS3, upgrading, and restoring FMS databases.

Ensure that you assign the appropriate server roles and role memberships to any user account that SOLUS3 used to upgrade the FMS database:

- Create a Level 5 Supervisor user in FMS (a user with Level 5 access rights), who will have the ability to Manage User Accounts. This category of user is granted full access to the features and functionality of FMS and can create user accounts. For more information on creating a user with Level 5 access rights, please refer to *Managing Users and Defining/Changing Access Rights* in the *Getting Started with FMS* chapter of the *Getting Started with FMS* handbook.
- When the Level 5 user is created in FMS, a SQL Server login is created automatically with a login name in the format `<database_name>_<FMS_username>`. For example, if the FMS database is called `fmsdb` and the FMS user is called `AbellA`, the SQL Server login is `fmsdb_AbellA`. Assign this SQL user membership of the following roles in the FMS database.

Required Server Roles	Required Role Memberships (for the FMS database)
dbcreator security admin	db_backup_operator db_ddladmin sims

For more information on adding an SQL user to these roles, please refer to the article on the Microsoft Developer Network.

Grant the SQL user permissions on the required schema objects in the FMS database.

Required Schema Permissions (in the FMS database)	
Schema Name	**Permission**
dbo	ALTER CONTROL DELETE EXECUTE INSERT REFERENCES SELECT TAKE OWNERSHIP UPDATE VIEW CHANGE TRACKING VIEW DEFINITION
sims	ALTER CONTROL DELETE EXECUTE INSERT REFERENCES SELECT TAKE OWNERSHIP UPDATE VIEW CHANGE TRACKING VIEW DEFINITION

For more information on granting permissions to schema objects, please refer to the following articles on the Microsoft Developer Network.

Additional Resources:

Permissions or Securables Page (http://msdn.microsoft.com/en-us/library/ms188515.aspx)
GRANT Schema Permissions (Transact-SQL) (http://msdn.microsoft.com/en-us/library/ms187940.aspx)

To log into the FMS database outside of the FMS application and to enable the upgrade of the FMS database via SOLUS3, you must reset the password of the SQL user. For more information on adding a SQL user to these roles, please refer to the article on the Microsoft Developer Network.

Re-installing an Agent on the Deployment Database, Deployment Service or Deployment Server UI Host Machines

If you need to re-install a SOLUS3 agent that has been removed from the Deployment Database, Deployment Service or Deployment Server UI, you must re-install the agent using the Deployment Service.

1. Select **Settings | SOLUS3** to display the **SETTINGS** page.
2. Select the **SOLUS** tab to display the **SOLUS SETTINGS** panel.
3. In the **Database instance** field, enter an extra character to the instance name, and then click the **Save** button.
4. In the **Database instance** field, delete the extra character, and then click the **Save** button again to force the DS to re-install the necessary agents.

Installing a SOLUS3 Agent using Group Policy

If there is a non-Windows firewall between the DS at the LA and devices at schools that do not have their own DS, the Windows Group Policy can be used to deploy scripts that will install the SOLUS3 agent on each device.

> *NOTE: Although Capita SIMS cannot provide bespoke scripts, using the **Export agent installer** button on the **System Configuration** page produces a default script that can then be amended.*

Any script deployed by group policy must perform the following tasks:

1. Create an installer log file name that will record installation information on each device. For example, create a file entitled `agent_install.log` in the `C:\Windows` folder of the device.
2. Run the appropriate msi installer from a network share with read access for Domain Computers.
3. Copy the following files from the folder on the DS (`C:\Program Files\Solus3\DeploymentService`)to the network share:
   - `SOLUS3AgentInstaller_x86.msi` (32-bit)
   - `SOLUS3AgentInstaller_x64.msi` (64-bit).
4. Pass the agent address to the agent installer. The default address is `net.tcp//localhost:52966`.
5. Pass the Deployment Service address to the agent installer. The default address is `net.tcp//<DS NAME or IP>:52965`. To view the DS address, select **Start | All Programs | SOLUS 3 Deployment Server UI | Settings | SOLUS3 | SOLUS**.
6. For each agent installation, pass a unique Global Unique Identifier (GUID) to the agent installer.
7. Copy the DS key file (`Solus3.Keys.DeploymentServer.Public.xml`) to the device.
8. Copy the DS key file from its default location (`C:\Program Files\Solus3\DeploymentService`) to a network share that has read access rights for Domain Computers.

Authorising and Deploying Revised Filesets for Statutory Returns

IMPORTANT NOTE: *Administrators must ensure that the SIMS user details and SIMS database are set up in* ***Targets****.*

In SIMS, filesets are used throughout the Statutory Returns area to facilitate the submission of an accurate return to a statutory body.

Occasionally, additions or corrections are made to these files, after a SIMS release, which are required for the forthcoming return. Filesets can be authorised and deployed to schools via SOLUS. The Import Fileset functionality can then be run by a user at the school who has the appropriate permissions. If you choose not to authorise and deploy filesets via SOLUS3, they will still be available for download from the My Account website.

IMPORTANT NOTE: *The report files are not always updated between releases. A newsfeed will be posted to the My Account website (https://myaccount.capita-cs.co.uk) (under* ***Notifications****) if updated files are available for import.*

TIP: To check which version of the fileset is currently in use, in SIMS select ***Routines | Statutory Returns | <census name>*** *to display the* ***Census Return*** *browser. The* ***Validation Fileset ID*** *is displayed in the header of the browser.*

Index