

# Installing and Configuring Cura

## Installation

Cura needs to be installed on an IIS server, as it is a web-based application. The recommended specs for Cura are:

- 2GB RAM
- 2 Cores

The Microsoft.Net Framework will need to be installed on the server hosting Cura. The server will also need Microsoft Internet Information Services (IIS) version 7.0 or later installed with the following features:

### Common HTTP Features

- Static Content
- Default Document
- HTTP Errors
- HTTP Redirection

### Application Development

- ASP .NET
- .Net Extensibility
- ASP
- ISAPI Extensions
- ISAPI Filters

### Security

- Windows Authentication

### Management Tools

- IIS Management Console
- IIS Management Scripts and Tools
- IIS 6 Management Compatibility
- IIS 6 Metabase Compatibility

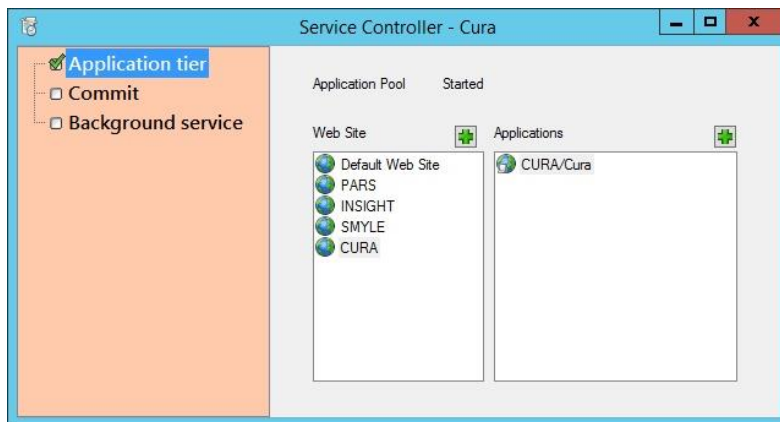
If you have a SIMS MIS then it is possible to allow staff to log in to Cura using their SIMS credentials, and have Cura automatically update its list of staff, students and parents from SIMS. For this, you will also need to install the SIMS workstation components onto the server.

To begin installing Cura, you will need to download a service pack from our website, [www.tascsoftware.co.uk](http://www.tascsoftware.co.uk). You can log in using the login details that were sent to you when you purchased Cura. If you have lost your details, please contact us on **01902 824281**.

Once you have logged in, click on the "Downloads" link at the top of our website. Download and run the latest Cura service pack on the server. Once you have accepted the licence agreement, the installation will unpack and begin.

The Service Controller will open, which is the program that installs and updates the Cura database and website. There are three options on the left side, each explained below. You should work through these from top to bottom.

## Application Tier

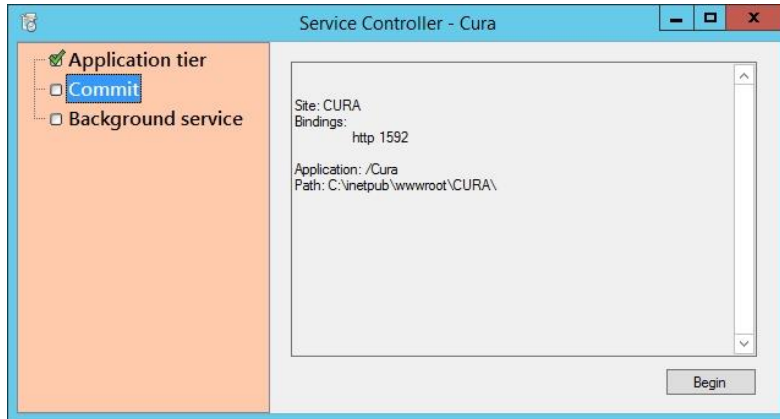


This node is used to configure a website. You can either use one of the existing web sites listed in the left hand panel, or add a new site. If you add a new site you will be asked to specify the site name, the listening port (which should not collide with any existing sites or services), and an SSL certificate if any such are present (or choose *none* if you are going to install this at a later date).

Additionally, you need to specify a folder on the IIS server where the application files will be stored. It is important to choose a location that the IIS user (NetworkService) will have permissions to read. **It is recommended to create a folder called CURA inside inetpub\wwwroot.**

Once you have chosen your site, you can add an application to that site. There are no options for this stage.

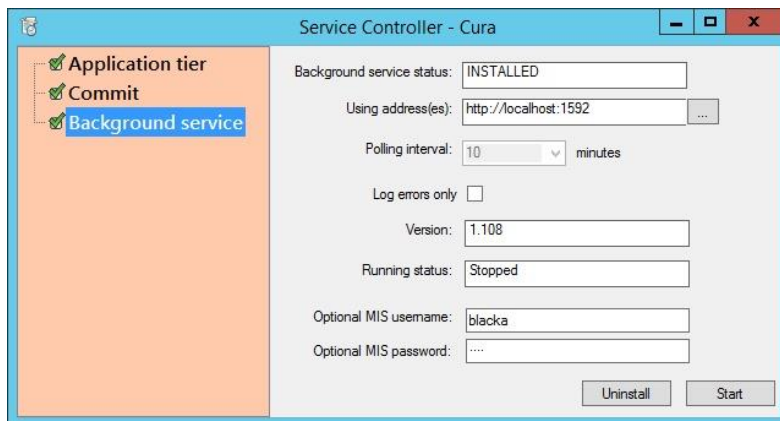
## Commit



Next click on the **Commit** node. Click the "Begin" button to commit the changes to your Cura application. This process needs to be performed each time a Cura service pack is run on the web server.

Once the commit process has completed, Cura will open in your server's default internet browser. If this happens, your update/installation has worked successfully. Take a note of the URL as this will be needed by users to access Cura.

## Background Service



### Optional MIS details

If you have a SIMS database then you can enter a SIMS username and password into these fields. This will enable staff to login using their SIMS username and password, instead of/ or their work email address and Cura password. Cura will also be able to periodically (3 times per day) scan SIMS to update its list of students and staff from the SIMS database.

### Running Status

This tells you whether or not Cura will be performing important automated processes. Follow the three steps below in order.

1. If the "Version" field includes the text "Update available" then click the "Uninstall" button at the bottom right.
2. If the "Running status" field is blank, click the "Install" button at the bottom right.
3. If the "Running status" field says "Stopped" then click the "Start" button at the bottom right.


## Creating an Admin Account

You should now have Cura installed on your server. The next step is to create an admin account which is used to manage the system settings, create accounts and manage permissions. To begin, go to the Cura login page using the URL obtained when running the service pack.

The Cura system only uses one admin account. There is a link at the top right of the login page which says "Register". This is used to create the admin account and once that account is created, the link will disappear.

Before creating your admin account, you should download an authenticator. You will need this to log in to Cura the first time, and you can configure Cura so that other users require an authenticator if desired. There are many free authenticators available, including one created by Google. If you want to use the Google authenticator, you can find instructions for it [on this webpage](#).

You will then need to enter the details for the admin account, including an email address and password. Once done, you will be given a QR code - scan this with your phone/mobile device or enter the 16 character code into an authenticator. You will need this to log in to Cura and you will not be given another QR code, unless you delete and recreate the admin account.



*Either:*

- scan the QR code into your authenticator using a QR reader
- type the 16 digit code into your authenticator
- take a note of the 16 digit code for later use

**jnwwtg3hobjkudl**

You will notice that the Network time and Server time are both displayed. The server time is the time on the server that you are currently using and the Network time is the current time taken from the Internet. The difference between the two times must be less than 60 seconds otherwise users will experience problems when trying to log in.

If the two times differ by more than 60 seconds then you need to change the time on your current server to reflect the Network time. If your current server's time is provided by another machine using the NTP protocol then you should update the time on that other machine.

Once the times closely match each other and the Authenticator on your phone or mobile device is matching the code shown on screen, you can click the link to be taken to the Cura login screen, where you will be able to log in.

## Configuring Cura

Now that you have created your admin account, log in to Cura. You will be taken to the System Settings page. You must enter your details into this page so that Cura can obtain your licence, before you will be able to access any other areas of the system.

### Proxy

The proxy section should contain your proxy details. For most schools, entering "DEFAULT" into the Proxy field will work, meaning the other three fields can be left blank. If this does not work, you will need to enter the correct proxy details for your school.

Once the details have been entered, click the Save button at the top right of the page and then click the "Test" link. Cura will attempt to communicate with **www.google.co.uk** and **www.tascsoftware.co.uk** and will then inform you of the results. If both connections are successful, your proxy is set up correctly.

### Site

Here you simply need to enter your LEA and School name. These details will be used to validate your licence.

### SMTP mail

The SMTP mail section needs to be configured in order for Cura to send emails. It is essential to enter these details as users will need to receive emails in order to activate their accounts. Emails are also required to send and receive alerts, and to reset forgotten passwords.

When you have entered your details, click the "Test" link to send a test email. You can specify an email address that the test will be sent to, and then Cura will show you the SMTP log results from that test.

### Licence

Once you have completed the three sections as above, click the Save button at the top right of the page and you licence details should appear in the licence section. If they do not, please contact our helpdesk.

## Mail header and footer

In this section you can add a header or footer that will appear on all emails sent via Cura.

## Clearance help test

When recording information, staff will be asked to specify a clearance level – this is a security level for the information that ranges between 1 and 5 (5 is the highest level of security). Each staff member will have their own clearance level. Staff cannot view the details about a piece of information if the clearance level of that information is higher than the staff member's own clearance level.

You can use the clearance help text option to add your own text next to the area where staff record the clearance level for information.

## Session timeout

These settings are used to automatically log users out of Cura if they have been inactive for a period of time. The session timeout in minutes option is the number of minutes before a user is kicked out.

The warning option is the number of minutes a user can be inactive before a warning appears on their page, prompting them to take action to prevent being automatically kicked out of Cura.

Once you are satisfied with your settings, click the Save button at the top right of the page and then click the Close button. This will close the System Settings page and take you to the Users page which allows you to configure permissions.

You can access the System Settings page at any time by clicking the cog icon at the top right of Cura.

## Setting Permissions for the Admin Account

You are now on the Users page where you can update permissions, set affinities or reset other users' secret codes.

Select the admin user using the tickbox on the left of the page, then click the "Open" button at the top right. This will open the permissions window. You should select the following options:

- Account manager
- Data importer
- Resource manager

You may also want to switch off the "Require two factor login" option. This will allow you to log in without using an authenticator to generate a PIN number.

Next click the "Save" button at the bottom of the window. This will update your permissions.

**admin**
✕

Approved:

Clearance: ★★★★★

Roles:

- Account manager
- Data entry
- Data importer
- Resource manager
- Resource consumer
- Report runner

Review severities: 
 1  2  3  4  5
   Limit to affinities

−
+

Simplified interface:

Require two factor login:

Now refresh your browser in order to apply your permission changes.

## Importing Children and Staff

The next step is to import staff and children into Cura. This is done using an xml file containing the details of the people to be imported. You can generate the xml files by running reports in the SIMS MIS. The format for these reports can be downloaded here:

<http://www.tascsoftware.co.uk/wiki/Cura/files/SIMS%20Exports.zip>

In order for staff to be imported into Cura, they must have an email address recorded in SIMS, which is marked as 'Main' and 'Work'. For pupils to be included, they must be currently On Roll.

When you save the files, the file extensions must be *.staff.xml* for the staff file and *.students.xml* for the students file e.g.

My\_Staff\_Export.staff.xml

My\_Student\_Export.students.xml

## The Import Process

First click the "Browse" button at the bottom right of the page. This will open a window where you can browse files on your computer - find the xml file you are going to use for the import. Once done, click the "Upload" button at the bottom right of the page. This will import the xml file into Cura, and the name of the file will be shown in the middle of the page.

Wait for 30 seconds, then refresh your browser or click the refresh button at the top left of this page. The file you imported will now have been replaced by two new files, one with a *.consumed* extension and the other with a *.log* extension. The *.consumed* file is a copy of the file that you originally uploaded. If Cura did not create accounts for any of the people in the xml file that you uploaded, the *.log* file will explain why.

Once Cura has completed the import, the existence of these files will not affect the users or children in your system. Therefore you can delete these files if you wish. To delete the files, first select them using the checkboxes next to their names. Once done, click the Delete button, which is a red cross found at the top left of the page.



## Setting Permissions for Staff

Now that you have imported staff members into Cura, you will need to assign permissions to them. To do this, go to the Users page.

One or more staff members can be selected using the checkboxes next to their photos. Once you have selected the staff member(s), click the "Open" button at the top right of the page. You will see a window where you can alter users' permissions.

### The Cura Permissions

#### **Approved**

By default, users are approved. This means that Cura will recognise them and allow them to perform actions in the system (as long as they have any other required permissions, see below). If a user is not approved, they will not be able to log in, regardless of their other permissions.

#### **Clearance**

The user's clearance level decides which pieces of information they are able to view. When a staff member records something in Cura, they will need to give a clearance level between 1 and 5. The higher the clearance, the more sensitive the information is. A staff member can record an incident using any clearance level however they will not be able to review incidents above their clearance level.

#### **Account manager**

This permission is only available to the admin account.

#### **Data entry**

This must be active for users to record Concerns, Meetings, Correspondances or Actions.

#### **Data importer**

This gives access to the import page, used to import children and staff into Cura.

#### **Resource manager**

Upload resources, such as contact forms and policies, for other users to download.

## Resource consumer

This allows users to download resources that have been imported into Cura (see above).

## Report runner

A Report Runner is allowed to run reports to analyse the data that has been recorded in Cura.

## Severity

Each recorded piece of information in Cura must be given a severity level between 1 and 5. The higher the severity, the more concerning the information is.

A user's severity range dictates which pieces of information they will be responsible for acting upon. Users will either need to act on every incident within their severity range (e.g. the Child Protection Officer may want to deal with all Severity 5 incidents), or only the incidents within their severity range that affect students they share an affinity with (e.g. a form tutor may only deal with incidents affecting students in his/her form).

If a user's severity range is not above 0, they will not have to act upon any incidents. Incidents that need to be actioned are dealt with via the home page.

## Simplified interface

The simplified interface is used for users who will never need to review any incidents. They can record information and run reports (if given the Report Runner permission) but not review anything that has happened. Users who are using the simplified interface will not see the home page. If they have the Data Entry permission, then their login will default to the Students page. Users who have been given a Review Severities range cannot also use the simplified interface.

## Require two factor login

If this option is selected then the user will need to use an authenticator on their phone, tablet or mobile device in order to login. This gives a greater level of security.

Once you have selected the permissions you want to give to staff, click the Save button and the permissions will be applied. Cura is now configured and ready for staff to use!