APPLICATION NOTE

AC500 USER MANAGEMENT WITH V3 CONFIGURATION AND HANDLING
## Contents

1. **Introduction** .................................................................................................................. 3  
   1.1 Scope of the document ................................................................................................. 3  
   1.2 Compatibility ............................................................................................................. 3  
   1.3 Further information’s ................................................................................................. 3  
   1.4 Cyber Security in the AC500 PLC family .................................................................... 3  

2. **User Management** .......................................................................................................... 4  
   2.1 User Management with Automation Builder .............................................................. 5  
      2.1.1 Project Encryption .............................................................................................. 5  
      2.1.2 User Management for Automation Builder ....................................................... 6  
   2.2 User Management at AC500 V3 PLC’s ....................................................................... 7  
      2.2.1 PLC General ...................................................................................................... 7  
      2.2.2 Working with OPC UA ..................................................................................... 14  
      2.2.3 User Management Visualization/Web Visualization .......................................... 26  
      2.2.4 User Management for FTP Server ..................................................................... 29
1 Introduction

1.1 Scope of the document
The AC500 V3 PLC’s support User Management for the Automation Builder Project and also for the PLC in different applications like OPC UA and Visualization.

1.2 Compatibility
The application example explained in this document have been used with the below engineering system versions. They should also work with other versions, nevertheless some small adaptations may be necessary, for future versions.

- AC500 V3 PLC
- Automation Builder 2.2.0 or newer

1.3 Further information’s
A further application notes is located here:

- AC500 V3 - Encrypt and Sign your Application

1.4 Cyber Security in the AC500 PLC family
Please be aware that we have White Paper for AC500 PLC family:

- White Paper
2 User Management

User Management gives the opportunity to have different rights for different user groups, e.g. a user group Operator is able to see all Values in a HMI system and give some commands to the process behind. Another user group Maintenance have the same rights but in addition the group has the Right to change Parameter which have influence to the function of the process or machine.

To avoid reading of user name and password from the Network it is recommended to use encrypted communication when inserting user name and password.

Working with AC500 V3 and Automation Builder V2 enables a couple of opportunities:

Automation Builder

- Encryption of a project
- Working with User Groups and Users within one Project

AC500 PLC

- General User management for one PLC (mostly Login)
- Encrypted Communication for Login
- OPCUA Server (different symbol sets for different User Groups, different rights on symbols for different Groups)
- Encrypted Communication between OPCUA Client and Server
- Web Visualization (different Rights for different Users)
- Encrypted Communication for Login
- FTP Server (Access to different Directories of the file system in the PLC)
- FTP or FTPS Security Mode
2.1 User Management with Automation Builder

2.1.1 Project Encryption

- In Automation Builder go to Menu Project
- Choose Project Settings
- Security

- Select Encryption and Password

Be aware: If you forget the Password, you have no more access to the project.
2.1.2 User Management for Automation Builder

User Management at Automation Builder is valid for the actual Project.

2.1.2.1 Adding User Groups and Users

Menu Project/Project Settings

In tab Users and Groups new groups and Users can be inserted.

2.1.2.2 Editing Permissions

Menu Project/User Management/Permissions

Permissions can be granted to the User Groups

CAUTION!
Be careful with changing Permissions!
2.2 User Management at AC500 V3 PLC’s

User management at PLC Side is available for

- PLC General
- OPC UA
- Visualization/Web Visualization
- FTP server

CAUTION!
If you have lost the administrator password, there is no way to recover it and the PLC must be send back for repair!

2.2.1 PLC General

2.2.1.1 Activate User Management

- Configure your Gateway
- Double Click to PLC Name in Device Tree
- Push the refresh Button
- You will be asked to activate the user management
- Select Yes to activate
• You will be asked for a Username and Password

• Insert the default credentials:
  o User name: “Administrator”
  o Password: “Administrator”

• Then you will be asked for a new Password

After doing this you get a Default user management System

Note: Be aware, that with an activated User Management always User name and Password is needed to connect to PLC.

2.2.1.2 Create User Groups and User

• Push “Add” in Groups Area
• Push “Add..” in Users Area

![Add User Interface](image)

• Fill in User Name and Password

![User Management Interface](image)

Be sure that the Refresh Button is activated, because all the User, User Groups and Access Rights will be transferred directly to PLC and will be saved only directly in PLC.

Actual PLC User can be seen in the Headline of the Dialog.

As long as no Power Cycle is made at PLC and Automation Builder was not closed and reopened you can connect without inserting Username and Password (same User).

To change User please use Menu Online

![Automation Builder Interface](image)
Next time you want Login, you will be asked for User Name and Password

2.2.1.3 Change Rights of User Groups

- Login as Administrator
- Select Access Rights

  - Select an Object and Select the Rights for the Different User Groups. Rights can only be given to Groups and not to User.

2.2.1.4 Working with encrypted Communication for Login

- To work with encrypted communication for Login the first step is to create a certificate.
• Double Click to this Security Screen Button

![Security Screen Button](image1)

• Login as Administrator

• If the Information Windows are empty push Refresh Button

• Go to Devices tab

• Select PLC_AC500_V3

• Go to the Right Window and select "Encrypted Communication (not available)" and push the upper yellow certificate button (Create a new certificate on this device)

![Certificate Button](image2)

• Choose 4096 as Key Length and a validity period and confirm with OK

• Creation takes about 2-3 Minutes

![Certificate Settings](image3)

• A certificate for Web Server was created as well

• Logout
- Now encrypted communication can be enabled

- Colored Line show the Encryption communication between PLC and engineering station

Note: First time after creating the Certificate, select Encrypted Communication and Login a window appears with a Question of Trusting the Certificate

CAUTION!
Be aware the certificates that was created in the security screen are self-signed certificates and should not be used in production environments. Only for testing purpose!

- Push OK and Login continuous
2.2.1.5 Remove User Management

- Login as Administrator
- Right Mouse click to PLC_AC500 and select Reset Origin Device

A confirmation screen comes up – Confirm with Yes

- Wait about 30s, you will be logged out
- Reboot the PLC
- Please go to IP Config Tool to set the IP address from your PLC. This will be reset during Reset Origin Device

CAUTION!
If you have lost the administrator password, there is no way to recover it and the PLC must be send back for repair!
Please contact your area sales manager for further information.
2.2.2 Working with OPC UA

Prerequisite to use User Management at AC500 V3 PLC’s together with OPC UA is to have an encrypted communication.

2.2.2.1 Create Certificate for OPC UA Server at AC500

In order to encrypt data and exchange it with the client safely, the server needs a certificate that the client must classify as trusted when a connection is established for the first time.

Requirement: The active path to the controller is set.

Click “View Security-Screen”:
- Select “Devices” tab
- Select the controller in the left view
- All services of the controller that require a certificate are displayed in the right view
- Select the service “OPC UA Server (not available)”
- Create a new certificate for the device. Click the icon 📄
- The “Certificate Settings” dialog opens
- Define the certificate parameters and click “OK” to close the dialog.

The certificate is created on the controller.

The next step is to download the certificate to the computer.

- Upload the Certificate to your PC
- Restart the PLC to load the certificate during power up
2.2.2.2 Configure an Encryption at OPC UA Client

- Start the “UaExpert” application

- Click “Add Server”
- The “Add server” dialog opens
- Insert IP address from the AC500 V3 PLC and confirm
- Switch to Tab Advanced

- Select UAexpert Setting
- Manage Certificates
Create a Certificate in UAexpert
• Fill out the form and confirm with OK

• The certificate will be shown

• Copy this Certificate to your PC

• Upload to AC500 V3 PLC into the **Trusted Certificates** folder

• Connect the OPC UA client to the PLC
• The certificate cannot be validated because it's a self-signed certificate.
  o Accept and Continue
• This is only an intermediate handling

• Push Ignore
- Check in UAexpert
- Settings
- Manage Certificates
2.2.2.3  Create Project with VARs

- Add Symbol Configuration to Application
- Push „Build“ Button
- Enable Symbol Sets
• Select symbols for Symbol Set “User_1”

• Add 2. Symbol Set “User_1” by pushing “+” Button and fill in Name

• Select Symbols for Symbol Set “User_1”
2.2.2.4 Match Symbol Sets with User

- **Select Symbol Rights**
  
  ![Symbol Rights Selection Diagram]

- **Push Refresh Button**

- **Give Access Rights for the different Symbol Sets to the User Groups**
  
  ![Access Rights Assignment Diagram]
2.2.2.5 Connect OPC UA Client

OPC UA Client can now connect with different Users

When a window appear: Push Ignore
<table>
<thead>
<tr>
<th>#</th>
<th>Server</th>
<th>Node Id</th>
<th>Display Name</th>
<th>Value</th>
<th>Catalog</th>
<th>Status Time</th>
<th>Status Time</th>
<th>Statuscode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>144311</td>
<td>46320</td>
<td></td>
<td></td>
<td>10386</td>
<td>2016-11-01T00:00:00</td>
<td>2016-11-01T00:00</td>
<td>Good</td>
</tr>
<tr>
<td>2</td>
<td>144311</td>
<td>46320</td>
<td></td>
<td></td>
<td>10386</td>
<td>2016-11-01T00:00</td>
<td>2016-11-01T00:00</td>
<td>Good</td>
</tr>
<tr>
<td>3</td>
<td>144311</td>
<td>46320</td>
<td></td>
<td></td>
<td>10386</td>
<td>2016-11-01T00:00</td>
<td>2016-11-01T00:00</td>
<td>Good</td>
</tr>
<tr>
<td>4</td>
<td>144311</td>
<td>46320</td>
<td></td>
<td></td>
<td>10386</td>
<td>2016-11-01T00:00</td>
<td>2016-11-01T00:00</td>
<td>Good</td>
</tr>
<tr>
<td>5</td>
<td>144311</td>
<td>46320</td>
<td></td>
<td></td>
<td>10386</td>
<td>2016-11-01T00:00</td>
<td>2016-11-01T00:00</td>
<td>Good</td>
</tr>
<tr>
<td>6</td>
<td>144311</td>
<td>46320</td>
<td></td>
<td></td>
<td>10386</td>
<td>2016-11-01T00:00</td>
<td>2016-11-01T00:00</td>
<td>Good</td>
</tr>
<tr>
<td>7</td>
<td>144311</td>
<td>46320</td>
<td></td>
<td></td>
<td>10386</td>
<td>2016-11-01T00:00</td>
<td>2016-11-01T00:00</td>
<td>Good</td>
</tr>
<tr>
<td>8</td>
<td>144311</td>
<td>46320</td>
<td></td>
<td></td>
<td>10386</td>
<td>2016-11-01T00:00</td>
<td>2016-11-01T00:00</td>
<td>Good</td>
</tr>
<tr>
<td>9</td>
<td>144311</td>
<td>46320</td>
<td></td>
<td></td>
<td>10386</td>
<td>2016-11-01T00:00</td>
<td>2016-11-01T00:00</td>
<td>Good</td>
</tr>
<tr>
<td>10</td>
<td>144311</td>
<td>46320</td>
<td></td>
<td></td>
<td>10386</td>
<td>2016-11-01T00:00</td>
<td>2016-11-01T00:00</td>
<td>Good</td>
</tr>
<tr>
<td>11</td>
<td>144311</td>
<td>46320</td>
<td></td>
<td></td>
<td>10386</td>
<td>2016-11-01T00:00</td>
<td>2016-11-01T00:00</td>
<td>Good</td>
</tr>
</tbody>
</table>
2.2.3 User Management Visualization/Web Visualization

- Double Click to Visualization Manager
- Click to User Management

![Image of User Management Visualization](image1.png)

- Click to “Create User management with default groups and users”

![Image of User Management Table](image2.png)

- Check if Groups and Users are OK for the Application

- Insert your passwords for the different Users
- Click to Settings

![Image of Settings](image3.png)

- Adjust Settings for User Management
Working with the User management within the Visualization need a Login.

E.g. Use a Button to Login at Start Page

Configure "Inputconfiguration"
Now each Element in the Visualization can be assigned to a dedicated User Group

Now only Admins can see the Button and execute the Action.
2.2.4 User Management for FTP Server

Adding an FTP Server to one of the Ethernet Interfaces gives a FTP Client the opportunity to have access to different Directories of the AC500 V3 with different Passwords.