

MorphoManager

Quick Installation Guide

Table of Contents

Prerequisites for MorphoManager	3
Computer Hardware Requirements:.....	3
Supported Operating Systems:	3
Installation	4
Configuration	5
Server Manager.....	5
Advanced Client Configuration.....	6
Initial MorphoManager Client Setup	7
Adding a Biometric Device Profile.....	7
Adding a Biometric Device	8
User Policy Setup.....	9
Wiegand Setup (IMPORTANT!)	10
User Management and Adding Users	11
Screen 1 – User Details	11
Screen 2 – Additional Details	12
Screen 3 – Wiegand Details (If a Wiegand Profile is set)	12
Screen 4 – Photo Capture	13
Screen 5 – Fingerprint Capture	14
Testing the Added Users	16

Prerequisites for MorphoManager

This section outlines the requirements for MorphoManager systems.

Computer Hardware Requirements:

Processor:	Dual Core CPU
RAM:	4 GB
Ports:	Three USB ports
Network:	100Mbps Ethernet port required for client/server connections.
Internet Access:	Required for updates. (If no internet access is available, updates can be installed via USB memory stick or CD Rom)

Supported Operating Systems:

- Microsoft Windows 8.1
- Microsoft Windows 8
- Microsoft Windows 7
- Microsoft Windows Vista SP1
- Microsoft Windows XP SP3
- Windows Server 2003 R2
- Windows Server 2003 R2 SP2
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Installation

There are two configurations for MorphoManager:

- Client and Server on the same PC

A PC can have both the client and server software installed. The server software needs to be installed first.

- Server PC and Client PCs

The server software needs to be installed on the server PC and the client software needs to be installed on each client PC that will connect to the server PC over a LAN or VPN connection.

The server software needs to be installed first.

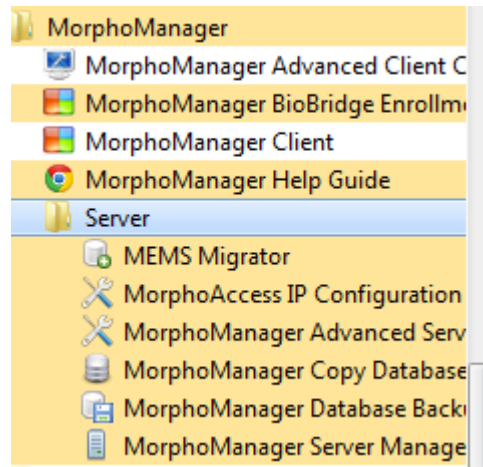
Install the Server and Client packages using the defaults given in the software. If the, "I accept the terms of the License Agreement" check off as below is not displayed, cancel the installation and reset the display to Windows default high resolution and regular or small display font.



At the end of the Server installation, it may suggest rebooting the PC. Do not reboot the PC at this point. However, at the end of the Client installation, it will again suggest rebooting the PC; please DO restart/reboot the PC then.

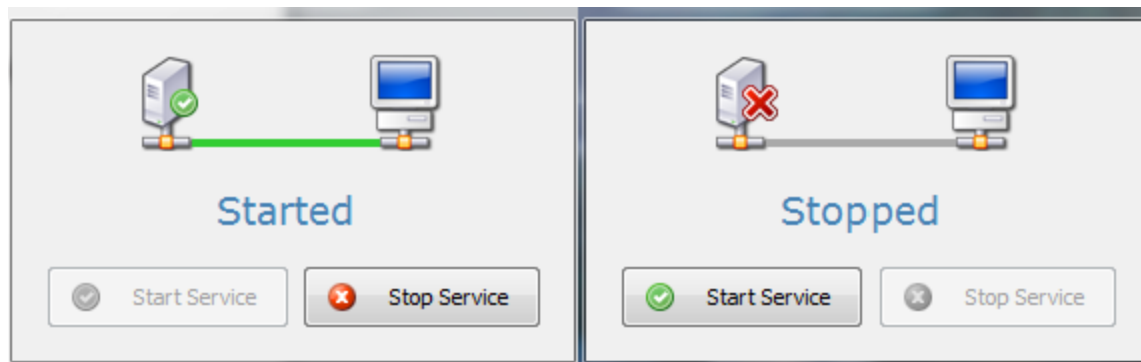
Configuration

After the installation of both the server and the client, under Start, All Programs, there should be a new MorphoManager group created with the following parts.



Server Manager

From the Server Group click on the MorphoManager Server Manager, it should already be running as below. If not, try starting it.



If the server is running, close the Server Manager and continue to Advanced Client Configuration. It's the first item in the MorphoManager group.

Advanced Client Configuration

For most installations, the default of **Automatic discovery** for the **Server connection type** will be suitable. Select the **Enable automatic login** option and fill in the Username: administrator (all in lower case) and the Password: password (all in lower case). This will save time while setting up and configuring MorphoManager and also speed demos and testing along.

Please note, in permanent installations, it is not recommended to leave the automatic logon enabled or to leave the default user name administrator and the password as password. Please refer to the MorphoManager

Select **Apply changes** button and then select the **Test** button. If using Automatic discovery, the current PC the server is installed on should be displayed. If there is another PC displayed or none, set the **Server Connection type** as **Local computer only**, click **Apply changes**, and then **Close**.

The screenshot shows the 'MorphoManager advanced client configuration' window. It is divided into three main sections: 'Server connection', 'Automatic login', and 'Server connection test'.

Server connection section:

- Server connection type:** A dropdown menu with 'Automatic discovery' selected. A tooltip shows the options: 'Automatic discovery', 'Manually specified', and 'Local computer only'.
- Broadcast port:** A text box containing '10.10.5.11'.
- Port:** A text box containing '42100'.
- Remoting channel type:** A dropdown menu with 'TCP' selected. A note next to it says '(Must match server setting)'.
- A button labeled 'Manage high availability server list' is located below the broadcast port field.

Automatic login section:

- Enable automatic login:** A checkbox that is currently unchecked.
- Username:** A text box.
- Password:** A text box.

Server connection test section:

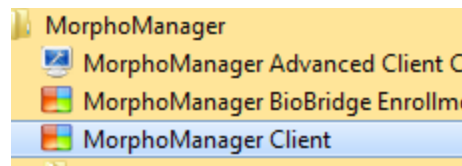
- A instruction: 'Click the test button below to discover servers'.
- A table with the following headers: 'Product', 'Version', 'Server connection point', and 'Server uptime'. The table body is empty.
- A 'Test' button is located at the bottom left of this section.
- A 'View errors' button is located at the bottom right of this section.

Bottom buttons:

- 'Apply changes' button
- 'Revert changes' button
- 'Close' button

Initial MorphoManager Client Setup

Select the **MorphoManager Client** program icon from Start> All Programs> MorphoManager to launch the application.



Adding a Biometric Device Profile

When the Client opens, select the **Administration** tab, then **Biometric Device Profile** from the items list, and lastly the **Add** button in the toolbar.

 A screenshot of the 'Adding Biometric Device Profile' window in the MorphoManager application. On the left is a sidebar titled 'Items' with a list of categories: Operator, Biometric Device Profile (selected), Biometric Device, Wiegand Profiles, User Policy, User Distribution Group, User Authentication Mode, Operator Role, Clients, Scheduled Reports, Card Template, Card Encoding Log, Event Log, and Exception Log. The main area is titled 'Adding Biometric Device Profile' and contains the following fields:

- Name: Text box containing 'Test 1'
- Description: Empty text box
- Configuration Mode: Dropdown menu set to 'Express'
- Wiegand Profile: Dropdown menu set to 'Automatically generated random 64 bit'
- Realtime logging enabled: Unchecked checkbox
- Log retrieval interval: Text box with '300' and '(seconds)' label
- Language: Dropdown menu set to 'English'
- Display name encoding code page: Dropdown menu set to 'Western Europe (Default) (ISO-8859-1)' with a note '(Applicable to MA500 series only)'
- Duplicate check on biometrics: Unchecked checkbox with a note '(MA 100, MA J, MA 500, MA VP and MA Sigma only. Only applicable to new user adds or rebuild operations)'
- MorphoAccess heartbeat interval: Text box with '30' and '(seconds)' label

 At the bottom right are four buttons: 'Back', 'Next', 'Finish' (with a green checkmark), and 'Cancel' (with a red X).

In order to create the most basic profile utilizing biometrics stored on the devices you wish to use, simply give your profile a name and click **Finish**. Please reference the MorphoManager User Manual for more detail on all the various properties that can be assigned to a Biometric Device Profile including the use of smartcards.



If you plan on using a Wiegand Profile, you will need to set the Wiegand Profile for the Biometric Device(s) here. The Wiegand Profile you choose for your devices must marry to the one being utilized for your users set in the User Policy section of this guide.

Adding a Biometric Device

Now that you have created your Biometric Device Profile you can add your Biometric Devices to the system. Select **Biometric Device** from Administration and then click **Add** in the toolbar.

The screenshot displays the MorphoManager interface for managing biometric devices. On the left, a sidebar lists various administration items, with 'Biometric Device' selected. The main area shows a table of biometric devices with columns for Name, Description, Location, Biometric D..., Status, and Tasks. A single device 'A' is listed with status 'Online'. Below the table, the 'Details' tab is active, showing fields for Description, Hardware Type (MA VP-Dual), Serial Number (11130086), Firmware version (3.3.8), Hostname\IP Address (10.10.6.221:11010), User Slots (0 / 5000), Time Zone ((UTC-05:00) Eastern Time (US Canada)), and Device Status (Online). A small image of a biometric scanner with a green checkmark is shown in the bottom right corner.

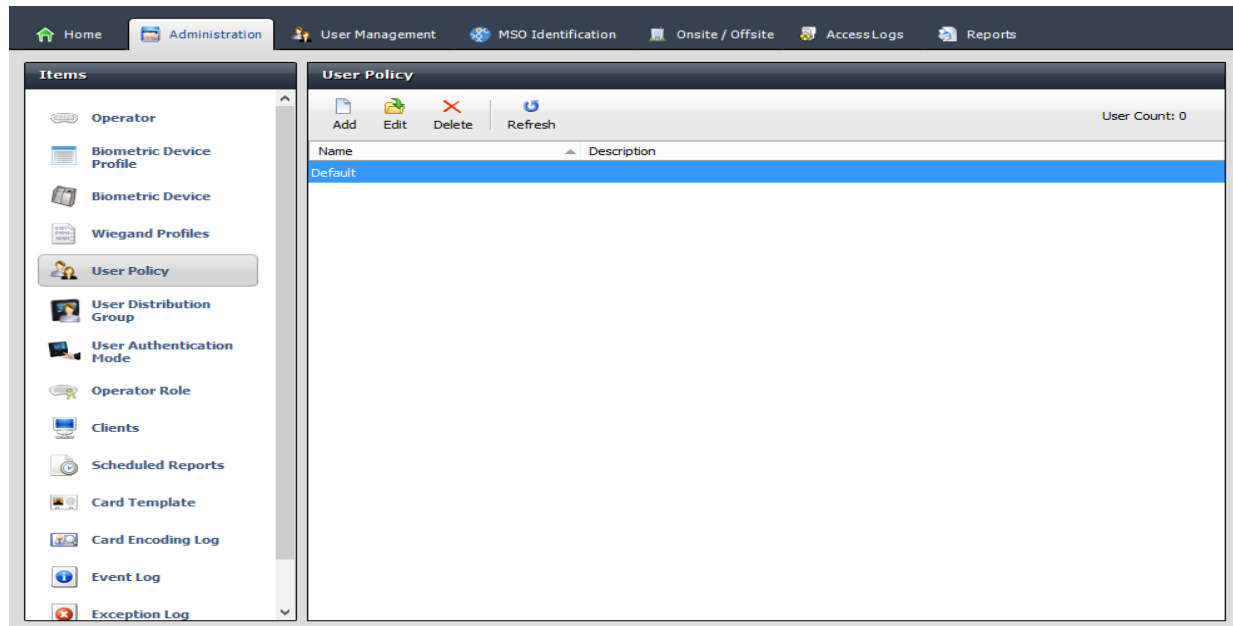
On the first wizard screen for adding a device fill out all mandatory information such as the, Name, Hardware Family your device is in, the IP address, and Biometric Device Profile you created. Once you have done so select **Finish**. The device should come online in the list of Biometric Devices.

Enter the details for this Biometric Device

Name:	Sigma Prox Unit
Description:	
Location:	
Asset ID:	
Export Value:	
Time Zone:	(UTC-05:00) Eastern Time (US & Canada)
Hardware Family:	MA Sigma
Hostname\IP Address:	10.10.3.25
Port:	11010
Biometric Device Profile:	Profile 1
Include in Time & Attendance Exports:	☐
Change User Onsite / Offsite Status:	☐
Onsite Key:	No Key
Offsite Key:	No Key

User Policy Setup

The next step will be to add your User Policy. Select the **User Policy** item on the Administration list



Select the **Add** icon. On the first wizard screen type in any name preferred and click **Next**.



If you plan on using a Wiegand Profile, you will need to set it here in order for the users enrolled in this User Policy to have a particular Wiegand Profile. The Wiegand Profile you choose for your users must marry to the one you utilize for your biometric access devices set in the Biometric Device Profile section of this guide.

Enter the details for this User Policy

Name:	
Description:	
Access Mode:	All Biometric Devices and Clients ☐ Allow MA 500 database selection during user enrollment
Time Mask Mode:	24 Hours, 7 Days a Week
Extended User Details:	☐ Display extended user details
Wiegand Profile:	Automatically generated random 64 bit
User Authentication Mode:	Biometric (1:Many)
Finger Biometric Enrollment Minimum Fingers:	Two
Preferred Finger One:	Left Index Finger
Preferred Finger Two:	Right Index Finger
Preferred Duress Finger:	Left Middle Finger

Please reference the MorphoManager User Manual for more detail on all the various properties that can be assigned to a User Policy including Wiegand Profile, Finger Biometric Enrollment Minimum, Fingers, Access Modes and User Authentication Modes.

Wiegand Setup (IMPORTANT!)

Many installations use backend systems that take the Wiegand signals from the MA units and feed them to an access control program/device that decides which people are allowed in and out at what times and through which doors. If being used for demonstrations or tests that do not use this feature, this requires no adjustment.

However, if the Wiegand output will be used, it will be set at the User Policy level from the Wiegand Profile drop down (See User Policy Setup screenshot on page 9). This drop down list reflects all of the Wiegand Profiles in the system. Users that are then added to MorphoManager will take on the Wiegand Profile of their assigned User Policy.

If you need to add a Wiegand Profile to the system, you can import them on the Wiegand Profiles section of Administration.

Name	Description	MA2G	MASG	M3DF
Automatically generated random 64 bit		Interpreted	Interpreted	Raw
CASI-RUSCO 40 bit	19 bit Facility / 19 bit Badge	Raw	Raw	Raw
HID Corporate 1000	HID Corporate 1000	Raw	Interpreted	Raw
ISO/IEC 14443 CSN 32 bit	32 bit Card Serial Number	Interpreted	Interpreted	Not supported
ISO/IEC 14443 CSN 56 bit	56 bit Card Serial Number	Interpreted	Interpreted	Not supported
ISO/IEC 14443 CSN 64 Bit	64 bit Card Serial Number	Interpreted	Interpreted	Not supported
Kastle 32 bit	Kastle 32 bit	Raw	Interpreted	Raw
Matrix 56 bit	54 bit User ID	Interpreted	Interpreted	Raw
OnGuard Wiegand 64	8 bit facility, 48 bit card number, 8 bit issue code	Raw	Raw	Raw
Standard 26 bit	8 bit Site/16 bit User code	Interpreted	Interpreted	Raw

User Management and Adding Users

Users are people who will have their biometric data (or minutia) sent to the selected Biometric Device for identification purposes for either access control or time and attendance. Select the **User Management** tab to access this area.

To create a new user, select the **Add** button on the Toolbar. This will display the User Wizard.

Screen 1 – User Details

Enter the details for the new user.

Home Administration **User Management** MSO Identification Onsite / Offsite Access Logs Reports

Adding User

Enter details for this User

User Policy: Default

First Name:

Middle Name:

Last Name:

Date of Birth: Use M/d/yyyy eg. 3/24/1986.

Back Next Finish Cancel

User Policy: Select the User Policy that this user will belong to. This is an important selection, as the User Policy will determine Biometric Device access as well as other access control and time & attendance settings.

First Name: User's first Name **(Required)**

Last Name: User's Last Name **(Required)**

Screen 2 – Additional Details

The screenshot shows the MorphoManager application window with the 'User Management' tab selected. The main area is titled 'Editing d w' and contains the following fields:

- Job title:
- Employee ID:
- Biometric device display name:
- Comments:
- MorphoAccess Database: (Only applicable for MA 500 with Xtended Licenses)

At the bottom of the form are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'. The status bar at the bottom of the window displays: 'Connected to tcp://10.10.5.11:42100/ Logged in as Administrator (System Admini Site ID: 4608-4BEB-AA9F-4B04-BFCB-23E9-5139-BADE Log Out Change Password'.

Screen 3 – Wiegand Details (If a Wiegand Profile is set)

Wiegand Values

User ID

A User ID can be added manually or a random one can be generated by clicking **Randomize**.

Screen 4 – Photo Capture



Position the person in front of a plain background so that all of their face is visible in the picture, similar to a passport photo. Once the user is positioned correctly click **Capture Photo**. Click on the image in the top left corner and drag towards the bottom right drawing a square around the part of the photo to keep. This can be done many times until the correct area is selected. Click **Accept Changes** to accept the changes if no camera is connected just click **Next**.

If the person is not available to have their photo taken, click **Person not at Camera**, to skip photo capture.



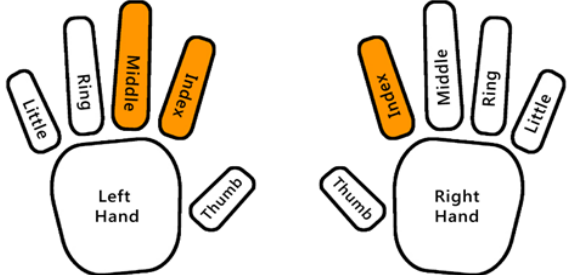
If the photo is not acceptable, click **Update Photo** to recapture the photo. Photos can be imported and exported using the corresponding buttons. Additional configuration options for the camera can be changed by clicking on **Configure Camera**.

Screen 5 – Fingerprint Capture

Adding User

Finger Biometric Enrollment

Click a finger to begin capture



Left Hand: Little, Ring, Middle, Index, Thumb

Right Hand: Thumb, Index, Middle, Ring, Little

Finger 1:

Finger 2:

Finger Duress:

The default fingers that the system suggests you enroll is defined in the User Policy settings (page 9) that your user is assigned to on the first wizard screen of this process. In this example both Index Fingers and the left Middle Finger are flashing orange based on the User Policy settings defining “Finger Biometric Enrollment Minimum Fingers”, “Preferred Finger One”, “Preferred Finger Two”, and “Preferred Duress Finger”.

You do not need to use these fingers as you can click on others.



The User Policy setup is usually set to expect at least two fingers to be enrolled so that the user will still have access should one fingerprint become unreadable due to minor events, such as knife cuts, Band-Aids etc.

Click on a finger. If the reader is connected correctly the following screen will be displayed.

Capturing left index finger



Have the user place their finger in the center of the scanner glass. You will then see the print appear on screen. There are four scans performed on each finger; the first three are used to create the biometric template. The fourth print is used for verification purposes. Below each enrollment image a color bar will

be displayed indicating the quality of the print as it is being captured. Green indicates quality is above recommended quality. Orange indicates the quality is above the minimum but below the recommended quality. Operators with administrative rights are permitted to accept fingerprints of this quality. Red indicates the quality is below the minimum.

Follow the instructions on screen. Green indicates ready to capture. Orange indicates that a finger is presented but the capture has not finished yet. Check the instructions to ensure the finger is placed correctly. Continue until all boxes are filled as in the image below.

Capturing right index finger



Once the enrollment is complete for both the fingers, you will see this screen. Captured finger quality is displayed on the right. In the event a user is not being recognized at any Biometric Device with one or both enrolled fingers, click **Clear <enrolled finger> finger enrollment** to allow re-enrollment.

Finger Biometric Enrollment

Click a finger to begin capture

Captured Fingers

Left middle finger enrollment metric: 84
 ✕ [Clear left middle finger enrollment](#)

Left index finger enrollment metric: 95
 ✕ [Clear left index finger enrollment](#)

Right index finger enrollment metric: 93
 ✕ [Clear right index finger enrollment](#)

Finger 1: Left index finger

Finger 2: Right index finger

Finger Duress: Left middle finger



Positive Identification and general performance of MorphoManager is maximized by the quality of the fingerprint captured during enrollment. MorphoManager has been designed to reject poor quality fingerprints; however it is still possible they may slip through.

The key to capturing a high quality fingerprint is to visually look for a clearly presented pattern that is centered and square with the right amount of pressure. Don't hesitate to retry the capture if you are unsatisfied. For assistance refer to the fingerprint capture guide in the MorphoManager User Manual. Click **Finish** to save the user or cancel to discard changes.

Testing the Added Users

Once enrollment is complete, the user's record is sent to any connected Biometric Devices authorized for that User and their User Policy. The Biometric Device unit will very briefly flash and then the fingerprint pad light will come on.

Presenting the enrolled finger will trigger a green flash and maybe hear a slight buzz and or click if the relay fires on the unit. In any event, select the **Administration** tab, select **Biometric Device**, and then select the unit the finger was presented to (it may be already selected if it is the only one present). Finally, select the **Get Logs** tab for that unit and confirm **Yes** to the confirmation message.

The screenshot shows the MorphoManager Administration interface. The top navigation bar includes Home, Administration (selected), User Management, MSO Identification, Onsite / Offsite, Access Logs, and Reports. The left sidebar lists various items: Operator, Biometric Device Profile, Biometric Device (selected), Wiegand Profiles, User Policy, User Distribution Group, User Authentication Mode, Operator Role, Clients, Scheduled Reports, Card Template, Card Encoding Log, Event Log, and Exception Log. The main content area is titled 'Biometric Device' and contains a table with columns: Name, Description, Location, Biometric D..., Status, and Tasks. A single row is visible with Name 'A', Status 'Online', and Tasks '0'. Below the table are tabs for Details, Logs, Queued Tasks (0), and Failed Tasks (0). The Logs tab is active, showing a table with columns: Accessed On, Access, User, and Key. A single log entry is visible: Accessed On '7/15/2015 2:50:40 PM', Access 'Granted', User 'D W', and Key 'No key'.

If the log tab is not displayed as above, select the **Show Details** icon in the lower right on the screen.