

# OVERS User Guide

*Oregon Vital Events Registration  
System*

**External Facility Administrator Edition**

Last Revised: January 2021

# Table of Contents

<b>Chapter 1: Basic Navigation</b> .....	4
System Requirements.....	4
Navigation Menu.....	4
Getting Started.....	5
Logging in.....	5
Home.....	6
Change Office.....	6
Change Your Own Password.....	7
Logout.....	7
<b>Chapter 2: Resetting Passwords</b> .....	8
Resetting Passwords.....	8
Looking up a user account.....	8
Resetting a user’s password.....	9
<b>Chapter 3: Options for Certifying a Record</b> .....	13
Installing an authenticator app.....	13
Microsoft Authenticator app.....	13
New Phone or re-installing the app.....	16
Steps for enrolling fingerprints.....	17
Add a Finger.....	18
Tips for Creating a Reliable Fingerprint Template.....	19
Test a Finger.....	20
<b>Appendices</b> .....	21
Appendix 1: Sample OVERS Enrollment Form.....	21

---

## Welcome to the OVERS User Guide

The Oregon Vital Events Registration System (**OVERS**) is a secure, web-based vital records management system that uses standard web navigation techniques and functionality. The application includes tools used to search and verify the quality and completeness of the data entered.

OVERS allows both State staff and state partners such as Medical Examiners, Physicians, Funeral Directors, Hospitalists, and Hospital Birth Information Specialists to initiate, update, and process birth, fetal death, and death records.

The Facility-level Administrator role was created to expedite the process of fingerprint enrollment and password resets for medical certifiers (physicians and/or hospitalists), birth attendants, and birth information specialists working in larger hospital facilities. Optionally, the facility administrator may also enter the death certificate information on behalf of the medical certifier, but shall **not** sign birth or death certificates.

Facility-level Administrators are designated by the facility with which they are associated and agree to perform the following tasks.

- Enroll fingerprints for new users and affirm their identity by reviewing their picture identification. Medical certifiers have a new option to certify records using an **authenticator app** instead of a biometric device.
- Reset passwords for users as necessary.
- Notify the OVERS Help Desk when staff leave your facility or when their contact information changes.
- *(optional)* Enter the death certificate information on behalf of the medical certifier

This step-by-step guide explains the techniques for assisting physicians with common issues such as resetting passwords, enrolling fingerprints, and setting up an authenticator app.

To learn more about entering death certificate information into OVERS, access the Death Medical Facility User Guide at:

<https://www.oregon.gov/oha/PH/BIRTHDEATHCERTIFICATES/REGISTERVITALRECORDS/OVERS/Documents/MedicalFacilityUserGuide.pdf>

## 1

# Basic Navigation

**In this chapter you will learn the basic navigation methodology of the application.**

## System Requirements

The **OVERS** application is web-based and does not require the installation of any standalone software, except for the drivers associated with the biometric device used for signing certificates. Most business computers should meet the minimum system requirements without further modification. At minimum, access to the application requires:

- Browser: Microsoft Internet Explorer if using a biometric device as that is the only browser compatible with the fingerprint reader.
- High-speed internet connection
- Operating System: Microsoft Windows 10; Mac X 10.4 or later running a PC emulator
- Adobe Acrobat Reader
- Fingerprint reader and associated device drivers for those wanting to use a biometric device. Or, medical certifiers can use an authentication app installed on their smartphone to certify records instead of a fingerprint reader.

## Navigation Menu

The OVERS application includes navigation controls commonly known to internet users. The Menu along the top of the screen displays on every page of the OVERS application. This Menu provides easy access to the different pages and information in the OVERS application. The Menu in the OVERS application changes dynamically according to the permissions allowed by a user's security profile. In other words, the system presents a different series of screens to an individual user based on the role they play in the system. An External Administrator will be presented with a different set of screens than a medical certifier.

The top Menu includes levels of menu groupings that will appear when you hover over. Each grouping also contains sub-menus.

### Avoid using the 'Back' button

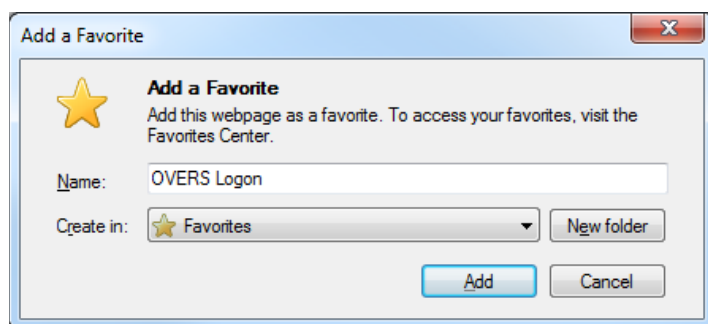
You may lose data entered if you navigate from one page to another using the 'back' button (located on the browser's tool bar). The OVERS application provides other tools for navigating from one page to another.



## Getting Started

### Creating an IE Favorite

The system administrator will provide you with a web address that will take you to the **OVERS** login page <https://or-vitalevents.hr.state.or.us/OVERS>. Once that page is displayed in your browser, select **Favorites > Add To Favorites** from the IE toolbar. This will launch the **Favorites** dialog shown below:



The **Name** field will automatically be filled in for you, but you may change it if you choose. To save the **Favorite**, click the **Add** button. You will now be able to select the **OVERS** website from your list of stored **Favorites**.

### Desktop Shortcuts

Another way to provide for quick access to the **OVERS** application is to create a **Desktop shortcut**. First, navigate to the login page, shown below. Then, from the IE toolbar select **File > Send > Shortcut to Desktop**. This will create an IE icon on your desktop that, when selected, will automatically launch Internet Explorer and open the **OVERS** login page.

### Logging In

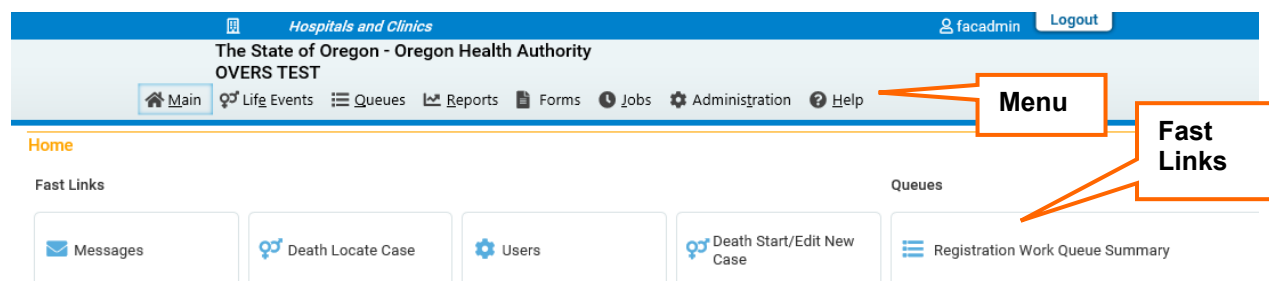
**OVERS** is a web-based application. If you are using a biometric device all of your work in the **OVERS** system must be done using Microsoft's Internet Explorer (IE) web browser. **Do not use Microsoft Edge**. However, you can use any browser if you are certifying records using an authenticator app.

Using either a **Desktop shortcut** or a pre-assigned IE **Favorite**, access the main **OVERS** login page.

Enter your assigned username in the **User Name:** field and your password in the **Password:** field and click the **Login** button.

## Home

After successfully logging in, you will be presented with a user specific **Home** page. Actions used most often are provided as Fast Links. All other available options are provided in the Menu along the top of the screen. Use the menu bar along the top of the page to navigate through the **OVERS** application.



The **Messages** section will not be pertinent to your work. However, the doctors you work with will find information about cases to be completed when they log in to their OVERS accounts.

The **Current Activities** section displays pending activities for your facility. It is important to review this area as it will display ALL pending death records for the entire facility. It will show every death record for all providers that need some type of action taken. For example, it will show cases for which medical certification has been requested from a doctor in your facility.

You can access the **Current Activities** section from the Home page by clicking the Fast Link for **Current Activities** or using the Menu by selecting **Main > Current Activities**.

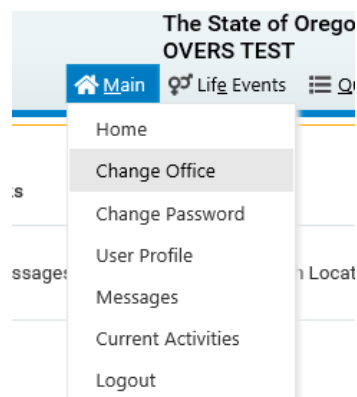
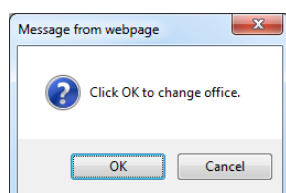
## Change Office

Some users may have access to records in more than one office or location. For example, a medical certifier may work at several facilities. In this case, the medical certifier would have one login, but would have access to multiple offices using that login. By selecting the **Change Office** link from the **Main Menu**, the medical certifier can quit working on cases in one facility and begin working on cases in the other.

### To change offices:

From any page in OVERS, select **Main > Change Office**

Click **OK** on the pop-up window.



At the login page, re-enter your password, then select the new office from the list. You may now work cases from the new location or office.

## Change Your Own Password

Typically, users are initially provided with a temporary password. This password will allow you to login to the **OVERS** system. However, you will be required to change your password before accessing the home page. Once you change the password, it will remain in effect for ninety days. At that time, you will be required to change your password.

You can also change your password at any time. From any page in OVERS, select **Main > Change Password**.

Enter your old or temporary password into the **Old Password** text box. Enter your new password into the **New Password** text box. Passwords must be between 8 to 26 characters in length, must start with a letter, and must contain a numeric digit. It can include a combination of uppercase and lowercase letters and numbers. Passwords are case sensitive. Re-enter the new password in the **Confirm Password** text box. Click the **Save** button.

## Logout

Whenever you are away from your desk or workstation, whether you're going home for the day or just going to lunch, you should always log out of the **OVERS** system by clicking **Logout** in the upper right-hand corner of OVERS.

## 2

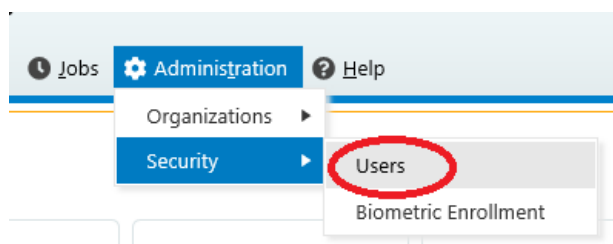
## Resetting Passwords

From time to time, it may be necessary to reset a password for a physician at your facility. The **Administration** feature of the **OVERS** application is used to reset passwords.

Only External Facility Administrators have access to the **Administration** features of the **OVERS** application. To perform **Administration** operations, log in, then select **Administration** from the Menu.

### Looking up a user account

The **OVERS** application features a simple, user-friendly interface for viewing and editing system users. To access this feature, select **Administration > Security > Users**.



The **Users** search page (shown below) will display. From this page, you can search for a specific user, and return a listing of all users in the system associated with your facility. Please note: as an External Facility Administrator you are not permitted to create a new user. **Only the State office will create new users.**

Search for a User

Username  Last Name  Office  User Type

Search Current Search All ~~New User~~

**Note: The ability to select the various Administration features is based on user security privileges. You may or may not have access to these pages.**

### Search Current

To search for accounts for active users within the system, enter either the **Username** or the user's **Last Name** and click the **Search Current** button:

Search for a User

Username  Last Name  Office

Search Current Search All New User

The result of this search will be a listing of all users whose Last Names contain "Test."



As seen in the search results table below, **2 Total Records** were returned by this search.

Search for a User Search Current Search All New User

Username  Last Name  Office

User Name ↑	Name	Office Name	Start Date	End Date
<a href="#">testdoc2</a>	Test, Another Doctor	Adventist Medical Center	07/15/2016	
<a href="#">testdoctor</a>	Test, Doctor	Adventist Medical Center	07/15/2016	

Total Records: 2

If an account is listed for an individual that is no longer employed by the facility, contact the OVERS help desk to have the account end dated.

Notice that each of the column headers in the above search results table are the color blue. Selecting any of these column header links will re-sort the results table according to that particular column's contents. The default sort order is by **User Name**.

Additionally, **Search Current** can be used with a combination of any of the three search criteria to yield very specific results.

### Search All

To return a listing of active and inactive user accounts at your facility, type in the name of your facility in the office field and click **Search All**:

Search for a User Search Current Search All New User

Username  Last Name  Office

## Resetting a user's password

Regardless of the search method employed, notice that the **User Name** displayed for each user is actually a blue link. Clicking the **User Name** link will open the user's **User Summary** page, enabling you to view or edit the user's setup.

Username	Last Name	Office
<input type="text"/>	<input type="text"/>	<input type="text"/>

Userid	User Name ↓	Last Name	Office
17528	<a href="#">ballida001</a>	Dzgo	Adventist Medical Center
21042	<a href="#">testdoc2</a>	Test, Another Doctor	Adventist Medical Center
18813	<a href="#">testdoctor</a>	Test, Doctor	Adventist Medical Center

Clicking the **User Name** link will open the summary page (shown below). Clicking **Update Login Information** will open a new window enabling you to make changes to the user's password.

From the **User Summary** page, you will only access the “**Update Login Information**” link.

**User Summary**

<b>User Id:</b> 30572 <b>User Name:</b> testdoctor <b>Password Expiration:</b> 10/13/2016 <b>Start Date:</b> 07/15/2016 <b>End Date:</b> <b>Logon Attempts:</b> 0	<b>Name:</b> Doctor Test <b>Title:</b> Doctor of Medicine <b>User Address:</b> 1234 Test Street Test, Oregon 97232 <b>User Mailing Address:</b> 1234 Test Street Test, Oregon 97232	<b>Work Number:</b> 123 456-789 Ext <b>Cell Number:</b> - <b>Home Number:</b> - Ext <b>Fax Number:</b> 987 654-321 Ext <b>E-mail:</b> facilityadministrator@test.com <b>Preferred Contact:</b>	<b>Medical License:</b> MD00000 <b>NPI Number:</b> <b>Funeral Director License:</b>
--	--	---	--

**Adventist Medical Center**  
Doctor Test is authorized to sign for the following events: Birth, Death, Fetal death

<b>User Type</b> Medical Certifier Total records : 1	<b>Office</b> <del>Adventist Medical Center</del> Total records : 1	<b>Roles</b> External: Medical Certifier Total records : 1	<b>Additional Business Functions</b> No data found.
--	---	--	--

~~Update Offices/Roles/Business Functions~~

[Biometric Enrollment](#)
[Return](#)

**Do not attempt to make any changes or update information related to the other links on the User Summary page. Making changes to pages other than the login information may cause problems with the user account. If other changes are needed, please contact the OVERS help desk**

After clicking on **Update Login Information**, you will see the **Update User** page shown below. Please note that you should not fill out every box on the page and do not click on any links along the left-hand menu. More details are provided below:

**Update User**

Select to Update a User Step 1 of 9

<ul style="list-style-type: none"> <li>1. User Account</li> <li>2. Name and Address</li> <li>3. Contact Information</li> <li>4. Licenses</li> <li>5. Office Affiliations</li> <li>6. User Types</li> <li>7. User Roles</li> <li>8. Business Functions</li> <li>9. Finish</li> </ul>	<p>1. User Account</p> <p><b>Username:</b> <input type="text" value="testdoctor"/></p> <p><b>Password:</b> <input type="password"/> Password and Confirm Password do not need to be re-entered unless they need to be modified.</p> <p><b>Confirm Password:</b> <input type="password"/></p> <p><b>Temporary Password:</b> <input type="checkbox"/></p> <p><b>Login(s) Attempted:</b> <input type="text" value="0"/> <a href="#">Reset</a></p> <p><b>Password Expires:</b> <input type="text" value="OCT-13-2016"/></p> <p><b>Start Date:</b> <input type="text" value="JUL-15-2016"/></p> <p><b>End Date:</b> <input type="text"/></p> <p style="text-align: center;"> <input type="button" value="Cancel"/> <input type="button" value="Back"/> <input type="button" value="Finish"/> </p>
---	--

---

**Username** – Do not edit.

**Password and Confirm Password** – You will not be able to see the current password for the user's account. If you need to provide the user with a temporary password, enter that password in these fields.

**Temporary Password** – When a user forgets or misplaces their password then a temporary password can be assigned. Placing a checkmark in the **Temporary Password** field will flag the account and require that the user change their password the next time they sign in.

**Login(s) Attempted** keeps track of the number of unsuccessful user login attempts. Once the count reaches 3, the account will be locked.

**Resetting a Password:** If the user knows their password and simply needs their account unlocked, click the reset button and have the user try logging in again. This will reset the number of Login(s) Attempted to 0. If there is anything other than a 0 in the Logins Attempted field then once you reset the password and click save, the field will reset to 0 again.

**New Password:** If this is a new user or the user doesn't know their password, you should enter a temporary password for the user in the **Password** and **Temporary Password** boxes and also select the **Temporary Password** check box. As described above, tagging a password as temporary will require the user to create a new password the next time they log into the system.

Instruct the user that you are resetting the temporary password and they will need to change the password the next time they log on to the account. Passwords may be between 8 to 26 characters long and must contain a numeric digit. Like user names, *passwords are case sensitive.*

Leave the **Password Expires** entry box blank. OVERS will automatically assign the expiration date.

Do not edit the **Start Date** or the **End Date**.

When all of the mandatory fields have been entered, click the **Finish** button to exit the **User Summary** page and save password changes. The user should now be able to log in with the password assigned.

### Update User

Select to Update a User

1. User Account

Step 1 of 9

- 1. User Account
- 2. Name and Address
- 3. Contact Information
- 4. Licenses
- 5. Office Affiliations
- 6. User Types
- 7. User Roles
- 8. Business Functions
- 9. Finish


Username:


Password:  Password and Confirm Password do not need to be re-entered unless they need to be modified.


Confirm Password:

Temporary Password:

Login(s) Attempted:

Password Expires:  

Start Date:  

End Date:  

Cancel

<< Back

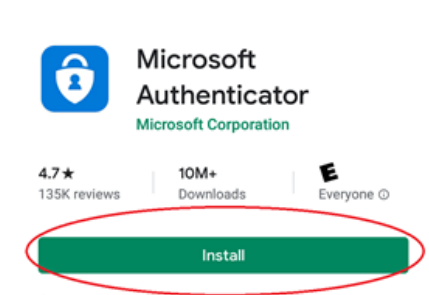
Finish

## 3

## Options for Certifying a Record

### Authenticator App

This option will allow medical certifiers to quickly certify records and amendments from any computer without the need for a biometric device. This new process will work with both Android phones and iPhones.

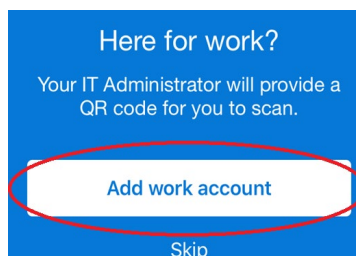


Search for an authenticator app on your phone. Authenticator apps can be found in the Google Play Store and the Apple App Store. In the app store, enter the word **Authenticator** in the search option and a list of authenticator apps will display. Select an app and tap **Install**. We recommend using Microsoft Authenticator. Apps from other companies should also work.


### The steps below are for the Microsoft Authenticator App installation.

Login to OVERS. Tap to open the authenticator app after it has installed. A Data Privacy Notice may appear. Click OK, select **Skip** when asked to **Add a personal account** and select **Skip** to **Add a non-Microsoft account**.

Click the **Add work account** button on the Here for work? page.



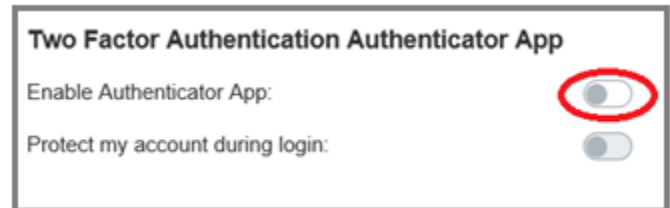
Allow the authenticator app access to your camera or video. This message may vary depending on your phone type.

 Allow **Authenticator** to take pictures and record video?

DENY **ALLOW**

Your phone camera will be activated in preparation to scan a QR code. A QR (Quick Response) code is a square bar code that your phone will read in OVERS to link your user information to the authenticator app. In OVERS, click on **Main and then User Profile**.

In the Two Factor Authentication Authenticator App section, click on the **Enable Authenticator App** slide bar.



A new window will open that has a QR code. Using the authenticator app, point your phone camera toward the screen to scan the QR code.

#### Authenticator

Improve the security of your account by enabling Two Factor Authentication. Just follow the simple steps below.

##### 1. Install Authenticator App on your phone

Install the Authenticator App on your mobile phone. The app is available on both Apple and Android phones and is published by either Microsoft or Google.

##### 1. Add to Authenticator App

Open Authenticator App and add by scanning the QR Code to the right.

##### 1. Enter the 6 digit code that the Authenticator App generates

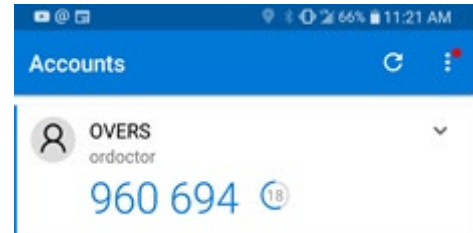
Verify that it is added correctly in the Authenticator App by entering the 6 digit code which the Authenticator App generates, and then click Enable.

Code:

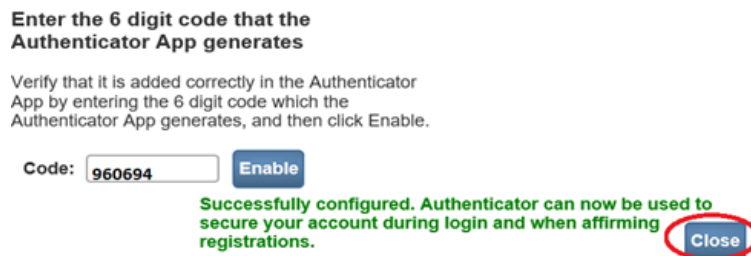


← QR Code

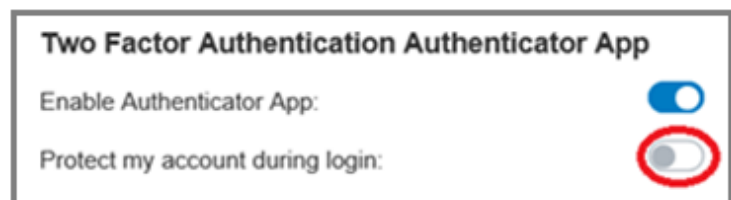
Once the code is successfully scanned, a 6-digit code will display in the app. **Enter the code with no spaces and click Enable.**



Click **Close** after receiving the Successfully configured message.



**If you don't want to enter a six-digit code every time you login, you must disable that option.**



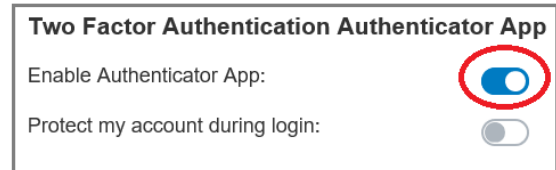
Click on the **Protect my account during login** slide bar to disable this option. When it is disabled it will show as grayed out.

The one-time set up to use the authenticator app is now complete. The app can be closed until needed to limit data usage.

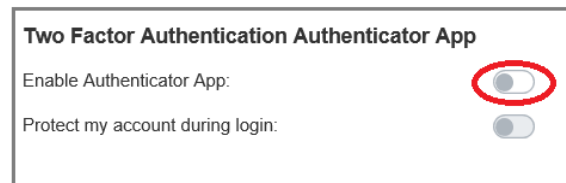
## New phone or need to re-install the app?

If the medical certifier gets a new phone or needs to reinstall the app, then the authenticator app will need to be disabled and then re-enabled in OVERS. Login to OVERS and click on **Main and then select User Profile.**

Click on the slide bar for Enable Authenticator App to disable it. Then click OK on the Confirm Message.



Click on the slide bar to re-enable the authenticator app. A new QR code will display. Follow the instructions on the previous pages to install the authenticator app if needed. Scan the new QR code with your phone camera using the authenticator app.





## Enrolling Fingerprints

From time to time, it may be necessary to enroll or re-enroll a physician's fingerprints at your facility. Fingerprints are used in the OVERS application as a digital signature for signing birth and death certificates. Only users who are approved to certify records may have their fingerprints enrolled. Medical certifiers also have the option to use an authenticator app to certify records. You can skip this step and continue on to page 13 if you choose to use an authenticator app.

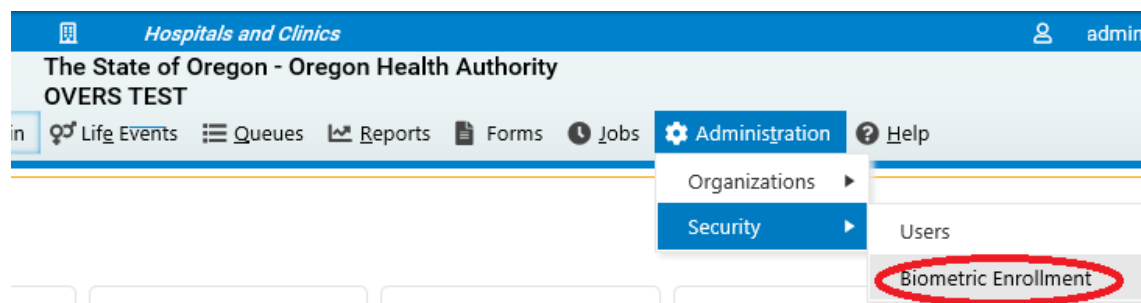
**All users enrolling their fingerprints must first provide you with picture identification or must be known to you as a signing authority (certifying physician).**

For a user to digitally sign a record using a fingerprint, a template of their fingerprint must first be stored in the OVERS database and associated with their user account. At the time of signing a record, the fingerprint template is compared to the signer's fingerprint. If the template matches the signer's fingerprint, then OVERS will accept the signature as a valid certification of the record. For certifiers who are new to using OVERS, we recommend a template be created for two fingers, and that each finger is enrolled multiple times so that the user will have a good fingerprint reading. The template is created by enrolling the user's fingerprints in OVERS.

### Steps for enrolling fingerprints

The **Administration** feature of the **OVERS** application is used for enrolling fingerprints

Only External Facility Administrators have access to the **Administration** features of the **OVERS** application. To access the fingerprint enrollment feature, select **Administration > Security > Biometric Enrollment**.



The **Biometric Enrollment** page (shown below) will display. From this page, the user must enter their username and password to access their fingerprint enrollment screen. After the user enters their username and password, click the **Search** button.

#### Biometric Enrollment

To proceed with the biometric enrollment process, have the user enter their username and password combination.

Username   
 Password

**Search**

You will be directed to the fingerprint enrollment page for the individual whose username and password were entered. You can verify that you are in the correct user account by checking the username that appears on the top of the screen.

#### Biometric Enrollment for testdoctor

**Add a Finger** **Test a Finger** **Biometric Setup Files** **Return**

**Be sure to enter fingerprints only for users who have signing authority (identified on the enrollment form). The username on the biometric enrollment page must belong to the user who is enrolling their fingerprints.**

If a user is new to OVERs, no fingerprints will be listed on their account. If you are **re-enrolling** fingerprints for a user, a listing for each enrolled finger will appear on the Biometric Enrollment page.

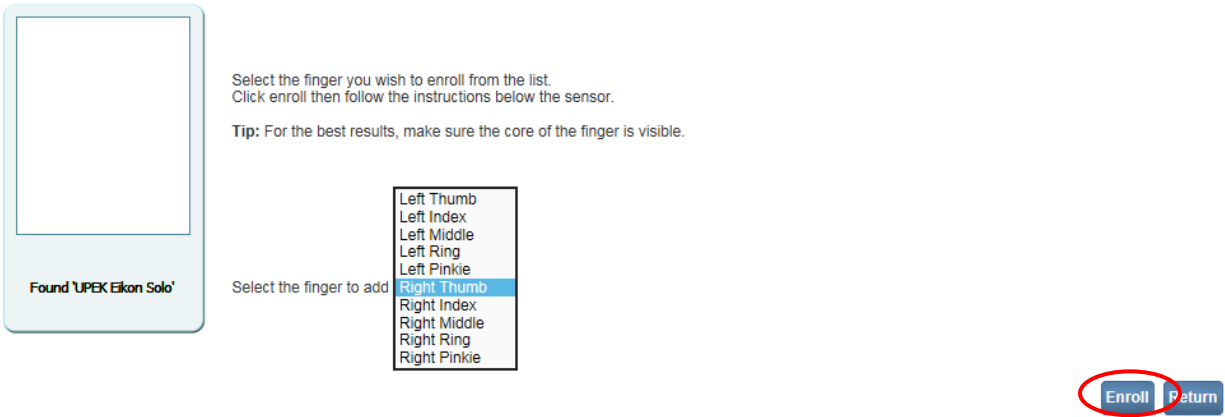
#### Biometric Enrollment for birthclerk

Finger	Chipset	Enrollment Date	
Left Thumb	AES3500	3/22/2013 3:42:55 PM	Delete
Right Index	AES3500	3/22/2013 3:36:32 PM	Delete
Right Ring	AES3500	3/22/2013 3:43:16 PM	Delete

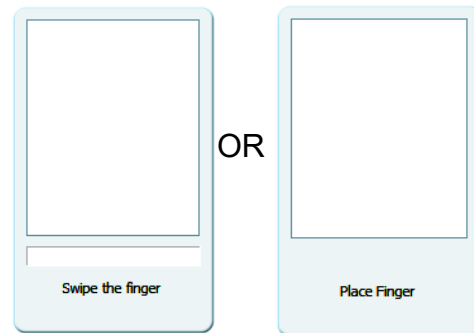
**Add a Finger** **Test a Finger** **Biometric Setup Files** **Return**

## Add A Finger

To enter a fingerprint template for a new user, click on the **Add a Finger** button. You will be directed to a new page. From the 'Select the finger to add' dropdown box, select the finger you wish to enroll. Next, click on the **Enroll** button.



Depending on the biometric reader your facility has (APC vs. Eikon Solo), the user will be prompted to either swipe or place the appropriate finger on the biometric device. To create a template of a finger, the finger will need to either be swiped along the surface of the reader or placed on the reader approximately 6-9 times to obtain a good reading.



## Tips for Creating a Reliable Fingerprint Template

With an APC Reader:

- Use the ridge at the top of the biometric device as a guide for placing the finger. The finger should lie flat on the reader and the top of the finger should rest just below the ridge. This ensures a 'cleaner' image of the print and is a reminder for the user where to place their finger when signing.
- Instruct the user to place their finger on the biometric device using moderate pressure and holding it in place long enough for the device to acquire a clear image (about 1 to 2 seconds).
- Lift and replace the finger approximately 9 times trying to place it in the same location each time. When the fingerprint has been registered, text will appear below the display window prompting the user to lift and replace their finger.



With an Eikon Solo Reader:

- It is easiest to have the user hold the device in their hand. Swipe the finger in a downward motion, keeping the finger flat, and apply a moderate amount of pressure.
- The user will continue swiping their finger on the biometric device. This process may have to be repeated up to 9 times before the system will have a clean image of the print to store.



When the enrollment is complete, a note will appear beneath the fingerprint image that says, "Template Created". You will automatically be directed back to the listing of fingerprints.

We recommend that the user enrolls 2 fingers, and that each finger is enrolled multiple times so that the user will have a good fingerprint reading. It does not matter which finger is selected from the dropdown. You will be enrolling the same finger multiple times, so the fingers you select from the dropdown don't matter. To add another finger, click on the **Add a Finger** button and repeat the process.

## Test a Finger

To test the fingerprints that you've just enrolled, click on the Test a Finger button located on the page that lists the enrolled fingerprints. On the Test a Finger page, you will be prompted to place a finger on the biometric reader. Make sure to only test fingers that have already been enrolled.

If the fingerprint is tested successfully, the screen will display a message that states, "Finger was identified as Left Index", for example. If the finger was not successfully identified the screen will display a message that says either, "unable to identify finger", "fingerprint verification failed" or "bad image".

### Biometric Enrollment for testdoctor



Place the finger to identify on the sensor.

For help troubleshooting fingerprint enrollment contact our helpdesk technical support at 971-673-0279.

# Appendices

## Appendix 1: Sample OVERS Enrollment Form



**OVERS Enrollment Form**  
Fax completed form to: 971-673-1201

Name: \_\_\_\_\_

Professional Title:  MD  DO  ND  PA  NP  CNM  LDM

Professional License Number: \_\_\_\_\_

Facility Name: \_\_\_\_\_

Work Phone: \_\_\_\_\_ Fax: \_\_\_\_\_

Work Email: \_\_\_\_\_

Private Individual Work Email (for password reset only): \_\_\_\_\_

Facility Address: \_\_\_\_\_

City: \_\_\_\_\_ County: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_

Facility Mailing address if different: \_\_\_\_\_

City: \_\_\_\_\_ County: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_

*I attest that the above information is true and correct to the best of my knowledge.*

Signature of Participant: \_\_\_\_\_ Date: \_\_\_\_\_

Enter doctor's medical license number.

Check 'medical certifier' box for doctors, NPs, or PAs. Check 'facility administrator' for admin. support.

Check the box next to your User Type or OVERS Role below. (\*Indicates signing authority)

**DEATH REGISTRATION**

Funeral Home User:  Funeral Director\*  Funeral Home Staff

Medical Certifier:  Medical Certifier\*  Medical Certifier Staff  Facility Administrator

Medical Examiner:  Medical Examiner\*  Medical Examiner Staff

Certification Preference:  Authenticator App  Biometric Device  Both  
*(The authenticator app option is available to Medical Certifiers and Medical Examiners only)*

**BIRTH REGISTRATION**

Birth User Type:  Birth Information Specialist\*  Birth Clerk Assistant  Hearing Screener

**COUNTY STAFF**

County User Type:  County Registrar  Deputy Registrar

Select how the user would like to certify records.

**CHS OFFICE USE ONLY**

CHS Official: \_\_\_\_\_ Date Account Created: \_\_\_\_\_ Username: \_\_\_\_\_

Info. complete  Setup in OVERS  Added to listserv  Sent email

**COUNTY, FACILITY ADMINISTRATOR OR CHS USE ONLY**

Two Types of Identification Shown: Photo ID \_\_\_\_\_ and \_\_\_\_\_

Date: \_\_\_\_\_

*(County Official/Facility Administrator: Read and sign) I have reviewed the identification documents of the above-named participant and they appear to be genuine. To the best of my knowledge, the participant named above is eligible to sign or certify vital records in Oregon.*

Signature of County/State Official/Facility Admin: \_\_\_\_\_ Print Name: \_\_\_\_\_

*County Official/Facility Administrator - Fax this form to the State office after fingerprint enrollment is complete.*

List one type of identification shown.

Sign your name

Print your name

**Fax completed form to OVERS at 971-673-1201**