Integrated User Verification
Customer Implementation Guide
2017-02-09
Confidential
Version 3.1
TABLE OF CONTENTS

Introduction ....................................................................................................................................... 2
  Purpose and Target Audience ...................................................................................................... 2
  About This Document .................................................................................................................. 2
  Commonly Used Terms .................................................................................................................. 3
  Implementation Time ..................................................................................................................... 3
Overview: Integrated User Verification (IUV) .................................................................................. 4
  User Verification, Single Sign-On Verification and IUV ................................................................. 4
    Benefits ........................................................................................................................................ 4
  Challenges ..................................................................................................................................... 5
How Does IUV Work? ........................................................................................................................ 5
What are the Next Steps? .................................................................................................................. 6
Building and Configuring IUV .......................................................................................................... 7
  The Work Flow............................................................................................................................... 7
Building Your Integration Application ............................................................................................. 8
  Registering an Authenticated Shopper with a WebStore ............................................................... 8
  Redirecting the Shopper to the WebStore ..................................................................................... 13
Configuring ELMS to Talk to Your Application ............................................................................ 14
  Accessing ELMS Administration .................................................................................................. 14
  Finding Your Account Number ..................................................................................................... 14
  Turning “ON” IUV ......................................................................................................................... 15
  Testing Options ............................................................................................................................. 16
Sample Code .................................................................................................................................... 20
Restoring Administrative Roles ...................................................................................................... 20
Support ............................................................................................................................................ 21
Introduction

This section covers the following areas:

- Purpose and target audience
- About this document
- Commonly used terms
- Implementation time

PURPOSE AND TARGET AUDIENCE

This document gives you detailed instructions for establishing a single sign-on mechanism between a Kivuto customer’s existing authentication system (such as an LDAP directory) and a Kivuto ELMS WebStore. This process is called Integrated User Verification (IUV).

This document is aimed primarily at ELMS Administrators or web developers who have been assigned to the User Verification Administrator role in ELMS.

ABOUT THIS DOCUMENT

Read this document in conjunction with the online help available in the ELMS Administration website. The following is a list of the chapters in this document:

- Overview of the IUV process
  - What is single sign-on and Integrated User Verification?
  - How does it work?
  - What are the next steps?
- Building and configuring IUV
  - The Work Flow
  - Building your integration application
  - Configuring ELMS to talk to your application
- Sample code
- Support
COMMONLY USED TERMS

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer</td>
<td>A Kivuto customer (such as a company or educational institution) that is using IUV to authenticate shoppers to use an ELMS WebStore. In the ELMS Administration website, a customer is defined as an organization.</td>
</tr>
<tr>
<td>ELMS</td>
<td>Electronic License Management System. The ELMS platform includes both ELMS WebStores and the ELMS Administration site.</td>
</tr>
<tr>
<td>ELMS Administration</td>
<td>The secure administration module in ELMS that contains functions to manage a WebStore as well as set up IUV. This module is accessible by authorized users only.</td>
</tr>
<tr>
<td>IUV</td>
<td>Integrated User Verification: a single sign-on mechanism between the customer system and ELMS</td>
</tr>
<tr>
<td>Shopper</td>
<td>User that is being signed in to an ELMS WebStore.</td>
</tr>
<tr>
<td>WebStore</td>
<td>A Kivuto ELMS e-commerce website that provides products for sale on behalf of the customer.</td>
</tr>
</tbody>
</table>

IMPLEMENTATION TIME

The implementation time required to set up IUV for your WebStore varies with the type of authentication mechanism your organization currently uses and the technical abilities of your developers. An average implementation time for most experienced software developers is a couple of hours.
Overview: Integrated User Verification (IUV)

This section covers the following areas:

- What is Single Sign-On and Integrated User Verification?
  - Benefits
  - Challenges
- How does it work?
- What are the next steps?

USER VERIFICATION, SINGLE SIGN-ON VERIFICATION AND IUV

Only authenticated users can order software through your WebStore. WebStore Administrators must define how their users are authenticated. This is referred to as *user verification methods*. There are many methods of verification that can be used to authenticate users, including email domain, user import and Integrated User Verification (IUV).

Single Sign-On (SSO) verification methods allow a user to enter the same id and password to log on to multiple related but independent sites and software systems. The user logs in once and gains access to all systems without being prompted to log in again. IUV is one method of SSO integration with ELMS.

A WebStore can have multiple verification methods defined, however only one SSO verification type can be active at a time. Therefore, a WebStore cannot use both IUV and Shibboleth as verification methods at the same time.

More than one instance of SSO verifications can be added for testing purposes, however only one of each SSO verification type can be in Testing at a time. Other verification types (such as User Import) can only be added once. Also, if an SSO is set to Testing and there is already a verification of that type in Testing, the current type will be set to Inactive.

As different applications and resources support different authentication mechanisms, single sign-on has to internally translate to and store different credentials compared to what is used for initial authentication.

BENEFITS

- Reduces password fatigue from different username and password combinations
• Supports conventional authentication such as Windows credentials (i.e. username/password)
• Reduces support costs due to lower number of help desk calls about passwords
• Promotes security on all levels of entry/exit/access to systems without the inconvenience of re-prompting users
• Reduces administrative costs since user administrators only have to manage user databases/lists in the parent organization. All SSO systems are fed from that system.

CHALLENGES
SSO provides access to many resources once the user is initially authenticated. As a result, it increases the negative impact if the credentials are accessed by other people and misused. Therefore, SSO requires an increased focus on the protection of user credentials and should ideally be combined with strong authentication methods.

SSO also makes the authentication systems highly critical. Failure or an inability to reach the authentication system (such as network failure) can result in denying access to any system unified under the SSO.

Because of these challenges when using ELMS with IUV, it is imperative that the customer’s SSO implementation be available or else shoppers will not be able to access the WebStore and order software.

HOW DOES IUV WORK?
The following is an overview of the steps required to perform integrated user verification:

1. **Shopper arrives at customer site:** If the shopper browses directly to the ELMS WebStore, when the shopper clicks the link to sign in, the WebStore redirects the shopper to the customer’s site. The shopper could also start from the customer’s site.

2. **Customer site authenticates shopper:** The customer’s site prompts the shopper for his or her credentials and authenticates the user using its authentication mechanism (e.g. an LDAP directory).

3. **Shopper initiates switch to WebStore:** The shopper indicates that he or she would like to go to the WebStore by clicking a link or button on the customer’s site.
4. **Customer site registers authenticated shopper with WebStore:** The customer’s site retrieves any additional information required about the shopper from its own data store and makes an HTTP GET call over Secure Sockets Layer (SSL) to a Kivuto URL passing relevant information about the shopper and a security key to identify the customer. *See Building and Configuring IUV for more information.*

5. **Customer site redirects shopper to the WebStore:** If the HTTP GET call is successful – based on a specific return code – the customer’s site redirects the shopper to the return URL. This action completes the verification process, signs the shopper in to the ELMS WebStore and displays the WebStore’s home page to the user.

**WHAT ARE THE NEXT STEPS?**

- **Build your integration application**
- **Configure ELMS to talk to your application**
Building and Configuring IUV

This section covers the following areas:

- The Work Flow
- Building your integration application
- Configuring ELMS to talk to your application

THE WORK FLOW

1. Shopper clicks Sign In link
2. Shopper enters username and password
3. Customer system authenticates shopper and gets required attributes
4. Make HTTP GET call to ELMS
5. ELMS returns response codes
6. Read/Validate Response Code
7. 200 SUCCESS
   - Shopper begins shopping!
8. 500 FAILURE (Kivuto issue)
   - 1. Display message to user
   - 2. Inform customer of issue via email.
   - Kivuto will automatically be informed of the issue and will resolve.
9. 400 FAILURE (Customer issue)
   - 1. Display message to user
   - 2. Send email to Customer Development Team
   - Customer Development Team must fix the problem and RE-TEST!
BUILDING YOUR INTEGRATION APPLICATION

Build your integration application using whatever web technology is common to your organization. Code samples written in C# and VB.NET 2.0 that include an aspx page used for testing the integrated user verification process, as well as ColdFusion and PHP examples are provided at the end of this document. See Sample Code for more information.

Building your integration application requires two steps:

1. Registering an Authenticated Shopper with a WebStore.
2. Redirecting the Shopper to the WebStore.

REGISTERING AN AUTHENTICATED SHOPPER WITH A WEBSTORE

To register an authenticated shopper with a WebStore, the customer site must do an HTTP GET over SSL to the following URL:


Note: This is not a redirect; this step must be performed on a customer server.

User Authentication Parameters

The URL to do the HTTP GET over SSL has several required parameters and several optional parameters. The call is made over SSL so the parameters are automatically encrypted. The following is an example of a call to register an authenticated shopper with the parameters supplied:


The required and optional parameters are outlined in Table [1] Base IUV Implementation Data.

Some WebStores have a unique setup with more than one member organization where shoppers may belong, or the IUV implementation supports more than one WebStore. Refer to the data defined for Table [2] Single WebStore With More Than One Organization Using the Store and [3] Single IUV Implementation Serving More Than One WebStore below for more details.
### Table [1] Base IUV Implementation Data

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>account</td>
<td>Yes</td>
<td>The account number assigned to your organization within ELMS.</td>
</tr>
<tr>
<td>username</td>
<td>Yes</td>
<td>A unique identifier that describes each user. Maximum 100 characters.</td>
</tr>
<tr>
<td>key</td>
<td>Yes</td>
<td>“Shared secret” generated within ELMS Administration. This key should be kept as secure as possible.</td>
</tr>
</tbody>
</table>
| academic_statuses    | Yes       | **Important:** This parameter and the default values available are intended to be passed by academic organizations. Corporate organizations may need to pass different parameters to indicate the eligibility of their users. Consult your account manager for details. A comma-delimited list of “user groups” to which the shopper belongs. These groups influence the shopper’s eligibility to order software. Each value listed must exactly match a valid user group code (e.g. do not send “student”; it must be “students”). Default user groups are listed below. Additional user groups can be configured (in ELMS Administration) and then passed as necessary. **The default user groups are:**  
  - students  
  - faculty  
  - staff |
<p>| email                | No        | Shopper’s email address. Maximum 100 characters.                            |
| last_name            | No        | The last name of the shopper. Maximum 50 characters.                        |
| first_name           | No        | The first name of the shopper. Maximum 50 characters.                       |</p>
<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
</table>
| shopper_ip     | No        | The IP address of the shopper’s computer. This is used to verify the identity of the shopper when they are redirected to the WebStore. Do not send this parameter when  
• The shopper’s IP cannot be guaranteed, or  
• The “Verify shopper’s IP address” is disabled in Verification – Settings section in ELMS Administration. |
Table [2] Single WebStore With More Than One Organization Using the Store

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
</table>
| member_org     | Yes**     | ** for single WebStores with multiple member organizations only Organization Code(s) of the specific member organization(s) that the user will be placed into. Note: These codes must be defined in ELMS. Make sure to work with your account manager to set up this data. Example: "My Organization" is the parent organization. It has two satellite organizations (e.g. School Of Nursing and School of Management). If you want to have only one WebStore for the entire organization but want to track which user belongs to which organization, then Kivuto will set up an organization for each entity. My Organization = "OrgA" School of Nursing = "OrgB" School of Management = "OrgC" Each of these organizations has their own member_org value, but the HTTP GET call will share a common key and account. What follows are the sample HTTP GET calls where 100001111 is the fictitious account number of OrgA:


You can create one IUV implementation that points to multiple WebStores. Each WebStore is tied to an organization.

The account number and key parameters of the HTTP GET call determine which WebStore the shopper is redirected to.
Validating Response Codes

SUCCESS
If the HTTP GET call to register the authenticated user succeeds, an **HTTP status code of 200 (OK)** is returned to the customer integration application and the body of the response contains a URL to which the shopper can be redirected. See Redirecting the Shopper to the WebStore.

FAILURE
If an error occurred in the Kivuto system, an **HTTP status code of 500** is returned to the customer integration application.

If an **HTTP status code of 500** error occurs, Kivuto recommends that your application code does the following:

- Send an email to the web development team informing them of the error.
- Display a message to the user that access to the WebStore is currently offline and someone is working on the issue.
- Have the web development team contact Kivuto for support at tac@kivuto.com

If an error occurred due to problems with the parameters passed, an **HTTP status code of 400** is returned to the customer integration application with one of the error messages listed in Table [4] Error Messages below.

If an **HTTP status code of 400** error occurs, Kivuto recommends that your application code does the following:

- Send an email to the web development team informing them of the error.
- Display a message to the user that access to the WebStore is currently offline and someone is working on the issue.
- Have the web development team fix the issue.

**Note:** If you need assistance from Kivuto Support to resolve any errors, make sure you have the detailed message below handy to help in further diagnosing the problems.
Table [4] Error Messages

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The required parameter [parameter name] was missing or was present in the query string more than once with different values.</td>
<td>Indicates that the parameter indicated by [parameter name] was missing or duplicated.</td>
</tr>
<tr>
<td></td>
<td>If more than one parameter is missing, there will be more than one message delimited with the pipe (&quot;</td>
</tr>
<tr>
<td>WebStore not found. Check caller IP address and WebStore system name (if passed).</td>
<td>A WebStore was not found that was configured with the IP address of the calling server. See Configuring IUV.</td>
</tr>
<tr>
<td></td>
<td>This error message may also indicate that the account parameter is missing from the URL.</td>
</tr>
<tr>
<td>Submitted key does not match the one configured for the WebStore.</td>
<td>The key passed does not match the key assigned to the customer. See Turning “ON” IUV.</td>
</tr>
<tr>
<td>One or more of the user groups specified in the query string does not exist.</td>
<td>One or more of the user groups passed for the shopper does not match a valid user group code.</td>
</tr>
<tr>
<td>One or more of the user group classes specified in the query string does not exist.</td>
<td>An unrecognized parameter was present in the query string. For future use, extra query string parameters are presumed to be user group classes.</td>
</tr>
</tbody>
</table>

**REDIRECTING THE SHOPPER TO THE WEBSTORE**

If the HTTP GET call described above succeeds, the shopper must be redirected to the WebStore URL returned in the response.

The following is an example of a URL returned in the response:

https://e5.onthehub.com/WebStore/Security/IntegratedSignIn.aspx?token=Q0FFThapS%2beRmWsigr40nDSzDPFs%2fpwpWjM0jzrlBfyuF3JzrlLzX6mg%3d%3d&ws=2fb0a48a-350a-dc11-bb1f-001372747fc5

If, after being redirected, there is an error completing the user verification at the WebStore, the following error will be displayed to the shopper:

*We were unable to sign you in to the store. Please try again.*
The following are possible reasons for this error:

- The time between registering the authenticated user via the HTTP GET call and the redirection to the WebStore exceeded 60 seconds.
- The shopper’s IP address is being verified and it does not match the shopper IP address passed by the customer server when registering the authenticated user. See User Authentication Parameters above for details.

CONFIGURING ELMS TO TALK TO YOUR APPLICATION

To configure IUV in ELMS, you must be a registered and active ELMS Administrator or a web developer who has been assigned to the IUV Administrator role in ELMS.

ACCESSING ELMS ADMINISTRATION

To access the ELMS Administration website from the WebStore:

1. Enter the URL of your WebStore into your browser.
2. Click the Sign In link in the top right corner of the page.
3. Enter your Username.
4. Enter your Password.
5. Click the Sign In button.
   Once you are successfully authenticated, you will be signed into your WebStore.
6. At the top of the page, click the Administration link to access the ELMS Administration website.
   A new window is displayed.

FINDING YOUR ACCOUNT NUMBER

The ELMS account number is a unique identifier for your organization. This number is required for the following reasons:

- To sign into the ELMS Administration website without going through the WebStore.
  
  Note: If you set up IUV and it is configured incorrectly, you will not be able to access the ELMS Administration website through the WebStore to make the necessary changes to correct the configuration. You can access the ELMS Administration website via a special sign in page.

- To set up IUV.
When you sign out of the ELMS Administration website, a different “Sign In” page is displayed. This sign in page is not branded. See below:

This page requests your Account Number, Username and Password. It provides quick access to the ELMS Administration website without having to go through the WebStore.

**To find your Account Number:**

1. Sign into your WebStore.
2. Click the **Administration** link.
3. From the Main menu, click **Organization**. The Organization Details page is displayed.
4. In the **Account Number** input field, note the Account Number.

You can sign in directly to the ELMS Administration website by going to [https://e5.onthehub.com/admin](https://e5.onthehub.com/admin) and using your Account Number, Username and Password of the Administrator account.

**TURNING “ON” IUV**

To turn on IUV in ELMS, you must first have Standard Integrated User Verification set up as a verification type.

Setting up IUV requires the following steps:
1. Defining IUV as the verification type
2. Configuring IUV

Defining IUV as the Verification Type

To define IUV as the verification type:

1. Sign in to the ELMS Administration website.
2. From the Main menu, click WebStore. The WebStore Details page is displayed.
3. Click the Verification tab. The WebStore Verification page is displayed.
   The list of currently configured verification types are displayed on the page
   
   **Note:** By default, “User Import” has been configured for new WebStores or a different verification type may have already been configured.

4. Click the check box beside any verification type that is **not** Standard Integrated User Verification and then click the “Delete” button.
5. Click the **Add** button. The User Verification Types page is displayed.
6. Click the check box beside Standard Integrated User Verification.
7. Click the “OK” button to save your selection.

For the purpose of testing, you can add more than one Standard Integrated User Verification (IUV) verification method. By default, when a new verification type is added the status is set to “Testing”.

**TESTING OPTIONS**

You can test the verification type while it is in ‘Testing’ status.

**To view your WebStore with only Testing verification types:**

1. From the Main menu, click WebStore. The WebStore Details page is displayed.
2. Click the Verification tab. The WebStore Verification page is displayed.
3. In the Testing Options section, select the **Test WebStore URL with only Testing verification types in effect** URL.
4. Copy the URL.
5. Paste the URL into a different browser than the one you are currently using.

All the orders placed using Test WebStore URLs will be test orders. This means that the Order Details page will display “*Test Order*” and will not display any product keys.
Verification method status:

- **Testing**: Verification type can be tested but is not visible to shoppers on your WebStore. Only one of each Single Sign-On verification type can be in Testing at a time.
- **Active**: Verification type appears on the WebStore. Only one Single Sign-On verification can be active at a time.
- **Inactive**: Verification type does not appear on the WebStore and is not being tested.

To change the status of your verification type to ‘Active’:
Click **Activate** in the Actions column. If there was a verification of this type that was already ‘Active’, it will become ‘Inactive’.

To change the status of your verification type to ‘Testing’:
Click **Change to Testing** in the Actions column. If there was a verification of this type that was already in ‘Testing’, it will become ‘Inactive’.

To change the status of your verification type to ‘Inactive’:
Click **Deactivate** in the Actions column.

You can have more than one active verification method at the same time, providing the verification methods belong to a different ‘Class’.

Configuring IUV

Once IUV has been defined for your organization, you must now configure it.

**To configure IUV for your organization:**
On the WebStore Verification page, click the **Standard Integrated User Verification** link. The User Verification Type page is displayed for Standard Integrated User Verification.

On the User Verification Type page, there are two tabs: Details and Settings.

**Details**
Do not change the default values for “Sector” and “Verifications Expire In”. Changing these values could break your IUV resulting in your end-users not being able to sign into the ELMS.
### Settings

The Settings page defines the customer information that is required by Kivuto. Table [5] Customer Information Required by Kivuto lists the information that is required to configure a customer for IUV.

#### Table [5] Customer Information Required by Kivuto

<table>
<thead>
<tr>
<th>Information</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Sign-in URL</td>
<td>Yes</td>
<td>URL of customer site page that will authenticate the shopper prior to redirecting to the Webstore, or URL of a page with a link that will direct the shopper to the Webstore. The Webstore will redirect the shopper to this URL when a user performs an action for which authentication is required such as adding a product to a shopping cart, or when a user elects to sign out of the Webstore. To allow the customer site page to distinguish between these cases, a parameter is added to the URL's query string. The name of the parameter is “action” and its possible values are “signin” and “signout”. Appropriate coding must be developed to handle each case above.</td>
</tr>
<tr>
<td>Calling Server IP Address List</td>
<td>No</td>
<td>List of IP addresses of customer servers that will make HTTP GET calls to register authenticated shoppers with a WebStore. The WebStore will verify that the IP of a calling server matches an IP address in this list. For assistance in determining what these addresses should be, see Determining Customer Server IP Addresses below.</td>
</tr>
<tr>
<td>Organization Account Number</td>
<td>Yes</td>
<td>The account number assigned to your organization within ELMS. This number is displayed here for use in the integration application.</td>
</tr>
<tr>
<td>Key</td>
<td>Yes</td>
<td>“Shared secret” used to verify the identity of the calling server. Generate the key by clicking the Generate button. The key will not be saved until you click OK or Apply.</td>
</tr>
<tr>
<td>IUV Administrator Email Address</td>
<td>Yes</td>
<td>Email address of individuals or a distribution list who will receive error messages from ELMS.</td>
</tr>
</tbody>
</table>
Verify shopper’s IP address | No | In some cases, the shopper’s IP address as seen by the customer’s server may not remain the same after the shopper is redirected to the WebStore. This may happen due to a firewall dynamically assigning external IP addresses. By default this is disabled. If the check box is checked, the WebStore verifies that the IP of the shopper is the same as the shopper’s IP as determined by the customer server.

Determining Customer Server IP Addresses
In some cases, it may be difficult to determine the correct values for the customer server IP address list. This may be caused by:

- Multiple IP Addresses
- Load Balancing
- Testing IP Address

**Multiple IP Addresses**
If the customer server registering authenticated shoppers is configured with multiple IP addresses, typically the correct IP address is one of the following:

- Server base IP address
- Web server IP address under which the HTTP GET call is being made

If you are unable to determine the correct IP address, contact your Kivuto technical account representative. We can determine the IP address by analyzing web log data.

**Load Balancing**
If there are several load balanced or clustered customer servers that will be registering authenticated shoppers, you can provide a list of IP addresses for all of them.

**Testing IP Address**
For developers or testers testing integrated user verification, you can supply the IP addresses of developer and/or tester workstations. When development and testing is complete, you can provide the production server IP addresses.
Changes to Customer Information

If any of the customer information discussed above changes, it is imperative that the IUV settings be updated immediately (or, if the WebStore is managed by Kivuto, that Kivuto is notified immediately).

Failure to make these changes could cause IUV to cease functioning and shoppers will not be able to access the WebStore.

Sample Code

Samples of the code required by a customer server to register an authenticated shopper and redirect the shopper to the WebStore are available in C#, VB.NET 2.0, ColdFusion and PHP.

Click the following URL for sample code:

https://software.onthehub.com/documentation/ELMS_IUV_Sample_Code.zip

Restoring Administrative Roles

IUV implementation creates a new account for each user of your WebStore. When a user’s new username does not match their old username, administrative roles are not passed from the old account to the new. As a result, some of your WebStore’s administrators may find that they cannot access the ELMS administration site when they sign in with their new IUV account.

Affected administrators have two options if they wish to continue acting in their previous administrative capacity.

1. Contact Kivuto’s Support Team and request that the administrative roles associated with their old account be assigned to their new account.

   Note: Depending on the role being requested, the request may have to come from the primary administrator of your WebStore (i.e. the individual under whose name your organization’s subscription was issued).

2. Continue to sign in using their old account credentials rather than through IUV. This can be done through the admin sign-in portal at: e5.onthehub.com/admin.
Support

If you have any difficulties with configuring IUV for ELMS or require technical assistance, send an email to tac@kivuto.com.

Include the following:

- Customer Name
- Contact Name
- Contact Email
- Contact Phone
- ELMS Account Number
- Detailed description of the problem or request for information