

# HarvardKey Application Integration Form

*Please submit this form to register a new application with HarvardKey for authentication, authorization and optional attribute release services. You can type directly into this document and use as much space as you need for your answers. Additional information and a glossary of terms are available on the* [*IAM website*](https://iam.harvard.edu/get-started/app-integration)*. If you are seeking to integrate a new instance/environment of an application where one or more environments are already integrated and the configuration of the new environment should mimic the existing environment, you do not need to complete this form. Simply submit a support ticket with the information outlined in the* [*IT Help Portal*](https://harvard.service-now.com/ithelp?id=kb_article&sys_id=476957dc47374d50566cf147536d436c)*.*

# Application Owner

|  |  |
| --- | --- |
| **Owning Department** Indicate the School/Unit and Department responsible for ongoing maintenance and support of the application |  |
| **Department Contact**  Provide a departmental email address (and phone number, if available) that will not change with staff turnover (e.g., [iam@harvard.edu](mailto:iam@harvard.edu)). |  |

# Application Contact Details

*Please provide at least one contact for each role below. A single person may fulfill more than one role; however, there should be at least two different names listed in conjunction with any application. All but technical contact must be Harvard staff.*

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Name** | **Email** | **Phone** |
| **Registration Manager**  Harvard employee requesting the registration. Responsible for maintaining the application and registration information over time. |  |  |  |
| **Technical Contact**  Developer(s) familiar with the details of the technical implementation. Point of contact in the event of a technical incident. |  |  |  |
| **Business Owner**  Responsible for sponsoring the implementation |  |  |  |
| **Additional Contact(s)** |  |  |  |

# About Your Application

The information you provide on this form will be kept as part of the permanent record for this application integration with HUIT IAM Services, so please take time to answer all the questions on the form clearly and completely. Thank you in advance!

|  |  |
| --- | --- |
| **Name of your Application** *Please provide the name your application is commonly known by. Include both full name and acronym where appropriate.* |  |
| **Purpose** *Please describe the purpose of this application* |  |
| **Technology** *What technology(**ies) were used to build the application?* |  |
| **Application URL**  *The URL(s) used by end users to access the application* |  |
| **ServiceNow Application CI**  *(e.g., CIAPP00331, for HUIT-owned applications)* |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Will your application support local application credentials parallel to HarvardKey? | |  |  |  |  | | --- | --- | --- | --- | |  | Yes |  | No | |
| If YES, please describe how they will be used (e.g., emergency “backdoor” access): | | |
|  | | |

# Application Risk and Recovery Levels

*Definitions and detailed information about data risk level and system risk level can be found in the* [*Information Security Policy*](https://harvard.service-now.com/ithelp?id=kb_article&sys_id=c79350a7db011b0cd1257ee5bf9619fe)*.*

**What is your application’s system risk level?**

|  |  |  |
| --- | --- | --- |
| |  | | --- | |  | | **L1 - Public Information** |
| |  | | --- | |  | | **L2 - Low Risk**: Harvard systems that if compromised would not result in significant disruption to the School or University operations or research and would pose no risk to life safety. |
| |  | | --- | |  | | **L3 - Medium Risk:** Harvard systems that if compromised could result in material disruptions to School or University operations or research; material disruptions or damage to non-critical applications or assets; potential material reputational, financial, or productivity impacts. No risk to life safety. |
| |  | | --- | |  | | **L4 - High Risk:** Harvard systems that if compromised could result in major disruptions to School or University operations or research; major disruptions or damage to critical applications or assets; likely significant reputational, financial, or productivity impacts; life safety impacts. |
| |  | | --- | |  | | **L5** - **Level 5:** Specific to Research security protocol requirements |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **What is your application’s data risk level?**   |  |  |  |  | | --- | --- | --- | --- | | |  | | --- | |  | | **L1** | Information intended and released for public use | | |  | | --- | |  | | **L2** | Low risk confidential; information that may be shared only within the Harvard community | | |  | | --- | |  | | **L3** | Medium risk confidential; information intended only for those with a “business need to know” | | |  | | --- | |  | | **L4** | High risk confidential; information that requires strict controls | | |  | | --- | |  | | **L5** | Reserved for research data only, as determined by IRB or Data Use Agreement |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | **What is your application’s recovery criticality?**   |  |  |  | | --- | --- | --- | | |  | | --- | |  | | **0 - Foundational** | RTO up to 30 mins | RPO up to 30 mins | | |  | | --- | |  | | **1 - Mission Critical** | RTO up to 4 hours | RPO up to 30 mins | | |  | | --- | |  | | **2 - Critical** | RTO up to 8 hours | RPO up to 30 mins | | |  | | --- | |  | | **3 - Important** | RTO up to 24 hours | RPO up to 24 hours | | |  | | --- | |  | | **4 - Non-Critical** | RTO up to 7 days | RPO up to 24 hours | | | ***Recovery Time Objective (RTO)*** *refers to the quantity of time that an application, system and/or process, can be down without causing significant harm to the business as well as the time spent restoring the application and its data.*  ***Recovery Point Objective (RPO)*** *refers to the amount of data that can be lost within a period most relevant to a business, before significant harm occurs, from the point of a critical event to the most preceding backup.* | | Vendor-Specific Questions  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | Is this a software-as-a-service (SaaS) implementation? | |  |  |  |  | | --- | --- | --- | --- | |  | Yes |  | No | | | ***If NO, skip to the next section****, “Unique Identifiers”. If YES, please answer the questions below in this section.* | | | | Who is the vendor? |  | | Where is the application hosted? |  | | Provide a link to any vendor documentation regarding integration with single sign-on (SSO): |  | | Does a contract exist at this time? | |  |  |  |  | | --- | --- | --- | --- | |  | Yes |  | No | | | If YES, which office approved the contract? | |  |  | | --- | --- | |  | Strategic Procurement | |  | Office of General Counsel | |  | Other: | |  | Unsure | | | Name of Harvard employee who signed the vendor contract |  | | |

# Unique Identifier

Which [Unique](https://iam.harvard.edu/reference-documentation-unique-identifiers) Identifier will you use?

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | NetID1 |  | UUID |  | EPPN |  | HUID |  | Other: |  |

1 Applications with external users (users who do not have a HUID) are required to use NetID as their unique identifier.

|  |
| --- |
| It is recommended that your application accept NetID as your unique identifier. If you selected any other option above, please provide your justification for consideration: |
|  |

# Authentication Protocols & Attribute Release

*HarvardKey supports a variety of authentication protocols. Information about the various protocols can be found in the* [*Selecting an Authentication Protocol*](https://iam.harvard.edu/selecting-harvardkey-authentication-protocol) *knowledge article.*

*Please indicate which protocol you intend to use and complete the section below that corresponds to the protocol.*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | CAS |  | OpenID Connect (OIDC) |  | SAML/SP/Shibboleth |

Please note that all URLs are registered against the University’s production environment (Prod/P-0) by default. Customers’ production, stage (P-1), test (P-2), and/or development (P-3) instances will all “run in Prod.” If there is a business requirement, customers may register by special request for the HUIT stage environment, which is generally used for testing changes to the authentication systems themselves.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **CAS or CAS-with-Attribute Release: Endpoint URL**  Please list the endpoint URL(s) for each environment you will be integrating:   * Do not include any path or context, wildcard, “/” or “/\*” at the end of the URL. * To protect a specific path or context on your server or instance, configure the CAS client on your server. Some examples of paths you can configure on your side are **https://myapp.harvard.edu/pages** or **https://myapp.harvard.edu/secure/\***.  |  |  |  | | --- | --- | --- | | Env. | Desc. (e.g., DEV, TST, QA) | URL | | P-0 |  |  | | P-1 |  |  | | P-2 |  |  | | P-3 |  |  |  CAS Attributes *HarvardKey can provide attributes to applications in the authentication assertion. Please review the* [*Attribute Spreadsheet*](https://iam.harvard.edu/attributes-available-applications-using-harvardkey-authentication-services) *and list the attributes you would like to receive in the assertion.*  **Please note:** the attributes you choose should align with the data and system risk levels of your application.   |  | | --- | |  | |
| OpenID Connect (OIDC) Please list the endpoint URL(s) for each environment that you will be integrating:   |  |  |  | | --- | --- | --- | | Env. | *Description  (e.g., PROD, DEV, TST, QA)* | URL | | P-0 |  |  | | P-1 |  |  | | P-2 |  |  | | P-3 |  |  |  OIDC Attributes *OIDC returns a limited set of attributes in the sub claim and profile. All attributes will be provided.*   * Sub claim uniquely identifies the user * Profile returns name, family\_name (sn), given\_name, middle\_name, nickname, picture, and updated\_at. * Email returns the user's email address (login name as opposed to official email)   *Configuration and validation of the OIDC protocol in a lower environment is strongly recommended. Once we set up your application, we will supply the OIDC Issuer URL, Client ID, and Client Secret to you.* |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | SAML/SP/Shibboleth: Entity IDSAML SP Signing and Encryption Our policy is to encrypt assertion responses. We expect the service provider (SP) metadata file (see below) to include the SAML signing and encryption certificate. **Signing and encryption certificates should have a minimum expiration of three (3) years,** consistent with InCommon Federation best practices. **Note**: self-signed certificates are acceptable for this purpose.  For information on obtaining and renewing encryption certificates, visit the [SAML Encryption Certificate KBA.](https://iam.harvard.edu/saml-signing-and-encryption-certificates)  If you cannot accept an encryption assertion response, please provide your justification for consideration:   |  |  | | --- | --- | |  | | | Do you need to use Name ID? | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  | | --- | |  | | Yes | |  | | --- | |  | | No | | | If YES, which attribute should populate the Name ID? |  |  SAML SP Metadata Please generate and submit an SP Metadata file with this form.  To get HarvardKey IdP production metadata, visit: <https://key-idp.iam.harvard.edu/idp/shibboleth>. The HarvardKey IdP metadata file does not require authentication and can be downloaded by any vendor.  **If you are unable to generate an SP metadata file and submit it with this form, please complete the section below:**   |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | Application’s entity ID(s) in URL form: |  |   Provide the Assertion Consumer Service (ACS) URLs for each environment you will be integrating. The ACS is the URL(s) to which the IdP should send the SAML/Shibboleth authentication response. Please note: There may be multiple ACS URLs for each environment.   |  |  |  | | --- | --- | --- | | Env. | Desc. (e.g., DEV, TST, QA) | URL | | P-0 |  |  | | P-1 |  |  | | P-2 |  |  | | P-3 |  |  |   If you are not intending to use SAML/Shibboleth POST binding, please indicate that here:   |  |  |  | | --- | --- | --- | | |  | | --- | |  | | I am not intending to use SAML/Shibboleth POST Binding | |  SAML Attributes  *HarvardKey can provide attributes to applications in the authentication assertion. Please review the* [*Attribute Spreadsheet*](https://iam.harvard.edu/attributes-available-applications-using-harvardkey-authentication-services) *and list the attributes you would like to receive in the assertion.*  **Please note**: the attributes you choose should align with the data and system risk levels of your application.   |  | | --- | |  | | |  | | | |
| Attribute Use & Justification *Attributes obtained through authentication are for purposes of* ***authorization, account provisioning, and facilitation of the end user’s session*** *only.*  Business need for requested attributes:   |  | | --- | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | Will attributes received in the assertion be stored in a database related to your application? | |  |  |  |  | | --- | --- | --- | --- | |  | Yes |  | No | | | If YES, describe how that data will be used (e.g., reporting, authorization of users to the service, etc.): | | |  | |  |  |  | | --- | --- | | *Applications using attributes to create a directory browsable by end users of the application must be in alignment with University* [*data privacy guiding principles*](https://huit.harvard.edu/privacy)*,* [*directory listing policy*](https://iam.harvard.edu/resources/listing-policy) *and* [*FERPA requirements*](http://provost.harvard.edu/files/provost/files/ferpa_overview.pdf) *and honor user privacy by allowing individual users to opt out or acknowledge upon login that this data will be visible.* | | | Will your application use the attributes it receives to create a browsable directory of users? | |  |  |  |  | | --- | --- | --- | --- | |  | Yes |  | No | | | If YES, will end users (non-administrators) of your application have the ability to view data about other users? | |  |  |  |  | | --- | --- | --- | --- | |  | Yes |  | No | |  |  | | --- | | **User Authorization** | | Select the user group(s) below that describe who should have access to your application.  For more detailed information on the population(s) contained within these groups, view the [Authorization Filter KBA](https://iam.harvard.edu/harvardkey-generic-authorization-filters-0). | | |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  | Faculty |  | Staff |  | Students |  | Alumni |  | Other HUID Holders |  | Public |  | | | | | |
| |  |  |  | | --- | --- | --- | | Based on the user group descriptions provided the [Authorization Filter KBA](https://iam.harvard.edu/harvardkey-generic-authorization-filters-0), please describe your population in greater detail (e.g., any active student; students and staff from a specific school; library borrowers or HSRs): | | | |  | | | |  | | | | What is the primary authorization method you will use for your application? | | | | |  | | --- | |  | | An application-specific Grouper group as an authorization filter (e.g., harvard:org:ca:huit:iam:apps:midas:authorized-users-midas)   |  |  | | --- | --- | | **Application Group Name:** |  | | | | |  | | --- | |  | | A list of named users within the application (local permission list) | | | |  | | --- | |  | | An LDAP or API-based query to integrate an authorization decision | | | |  | | --- | |  | | Active Directory Groups | | | |  | | --- | |  | | Alseta | | | |  | | --- | |  | | Other, **Please describe:** | | | Authorization Filter All applications integrated with HarvardKey are required to have a group authorization filter to ensure that only current affiliates gain access. If you selected **“An application-specific Grouper group”** as your primary means for authorization, SKIP to the “External Users” section. Otherwise, review the list of filters on the [Authorization Filter KBA](https://iam.harvard.edu/harvardkey-generic-authorization-filters-0) and indicate in the box below which filter you would like us to use for your target population(s). If no appropriate filter exists, the IAM team will work with you during the consultation to create a new application-specific filter or generic authorization filter where appropriate.  Please note: generic filter you select has to align with the risk level of your application (L4 -> Red Tier, L3 -> Orange Tier, etc.). If the users from lower assurance tier can only see their own data and do not have privileged access, you can select lower assurance tier filter to go with higher risk level (e.g. L4 with Orange Tier).  If you need to allow access to test identities or users with privileged access, you will need to create an application-specific filter comprised of reference group(s)/tiers PLUS a managed folder for those test identities and other users who would not meet alignment criteria.   |  |  | | --- | --- | | I wish to use the following generic authorization filter for my application: |  |   *Or*   |  |  |  | | --- | --- | --- | | |  | | --- | |  | | An appropriate authorization filter does not exist for my application. Please assist me in creating a new filter. | | |   *If alumni will have access to your application, you need to obtain approval from Harvard Alumni Association to implement a filter that includes Alumni. See the* [*IT Help Portal*](https://harvard.service-now.com/ithelp?id=kb_article&sys_id=12dd722c1bba49d0485411b6bc4bcb5a) *for information on the process for obtaining approval.* |

# External Users (non-HUID holders)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Do you expect users who do not have a HUID to access your application? | |  |  |  |  | | --- | --- | --- | --- | |  | Yes |  | No | |

If **No**, skip to the next section. If **Yes**, your application will need to be integrated with HarvardKey Light.

To what **Return URL** should HarvardKey Light users be directed:

|  |
| --- |
|  |

# Single Sign-On (SSO) Configuration

HUIT can configure your implementation to force authentication at every login (not use SSO functionality). In this case, users will be prompted to provide their login name and password every time they seek access to your application, even if they have recently provided these credentials to another application within the HarvardKey authentication system. This type of non-SSO configuration is appropriate for applications managing sensitive data (e.g. financial, personally identifiable) as well as applications with a high probability of being accessed through public computers.

SSO is enabled as a default setting. If your application should NOT allow SSO, indicate it here:

|  |  |  |
| --- | --- | --- |
| |  | | --- | |  | | Do not allow SSO for this application |

Please note: HarvardKey standard session time is 8 hours (any user is automatically logged out of the application after eight hours). If your application has a way to configure application session lifetime, you should make sure it does not exceed the session allowed by HarvardKey. The two work independently and if they differ it can cause confusion for end users. For more detailed discussion of sessions, single sign-on (SSO) and single logout (SLO) visit the [*IAM website*](https://iam.harvard.edu/harvardkey-integration-services-session-timeouts).

If your vendor supports Single Logout (SLO), please refer to the [Session Timeouts KBA](https://iam.harvard.edu/harvardkey-integration-services-session-timeouts) to view your session options.

# Multifactor Authentication (MFA) Configuration

By default, HarvardKey authentication services requires MFA for all users except **alumni** and **delegate payers.** Application owners may choose to require MFA for all users, including these populations which are generally exempted.

|  |  |  |
| --- | --- | --- |
| |  | | --- | |  | | Require MFA for all users of this application including alumni and delegate payers |

By default, HarvardKey MFA allows SMS (text message) and phone calls for verification in addition to more secure methods such as Push, Mobile passcodes, Touch ID and Hardware tokens. Application owners may choose to limit MFA verification to the more secure methods by requesting a restrictive MFA policy. (This is contractually required by some vendors including Salesforce.)

|  |  |  |
| --- | --- | --- |
| |  | | --- | |  | | Assign the restrictive MFA policy to this application to limit MFA verification methods |
| Acknowledgment & Signature *By signing below (or by submitting this form from your Harvard email address) you certify that you have read the following important information and understand the impact for all your application instances that will be registered with HarvardKey services:*   * I certify that I fully understand that the only pages to which users may be redirected for entering their authentication credentials (e.g., ID and password pair) are the official University login pages * I acknowledge that the user must be redirected to these pages and the pages must not be presented to the user via web frames or any other method * I acknowledge that under no other circumstances may a web page be deployed that requests the user to enter Harvard University authentication credentials * I understand HarvardKey credentials never expire, and users will still have a working ID and set of credentials even if they have no active roles at the University * I understand that data provided in the assertion must not be distributed beyond the local system, and must only be used for the purpose requested in this application * I certify that the answers I have provided in this form are accurate, to the best of my ability * IAM regularly assesses authentication and authorization service offerings to ensure alignment with best practices and may retire a service. IAM will provide at least 12 months’ notice before retiring a service. If the service I am using is slated for retirement, I acknowledge that we will migrate to one of the supported offerings within the retirement period. | |
| ***Signature:*** | |
|  | |
| *If you are submitting this form from a harvard.edu email account, this signature is not required* | |
| Please submit this form and your SP metadata file (for SAML integration) to [iam\_help@harvard.edu](mailto:iam_help@harvard.edu).  A member of the team will contact you following submission to discuss next steps. | |

*Updated: 02/27/2024*