



MAXIENT TECHNICAL GUIDANCE

Updated March 25, 2022

As fully vendor-hosted software-as-a-service, Maxient requires only limited involvement from your campus IT staff. That involvement is focused on connecting Maxient with your campus information system and campus-based authentication services. Most campus IT departments are very busy. To ensure they have adequate time to complete their part of your Maxient implementation, **please provide this document to your campus IT team at your earliest possible opportunity.**

Maxient's integration with your campus IT infrastructure is most commonly one-way, ensuring that the application can never adversely impact your campus ERP data. We currently support three (3) data feeds, the specifics for which you will find below. It is preferable that all three feeds be available from the outset, but not essential; phased implementations for feeds #2 and #3 are perfectly acceptable. Be advised that feed #1 is required as part of your service agreement with Maxient.

Table of Contents

UNDERSTANDING HOW WE USE THE DATA FEEDS	2
FEED #1: DEMOGRAPHIC DATA	2
FEED #2: SCHEDULE DATA	4
FEED #3: ID PHOTOS	5
TRANSFERRING YOUR FEEDS TO MAXIENT	5
OPTIONAL BACKFEEDS TO YOUR CAMPUS	6
AUTHENTICATION	6
EMAIL AND SPAM FILTERING	7
FREQUENTLY ASKED QUESTIONS	8
Appendix 1 – Additional Campus Based Authentication Guidance	15
Appendix 2 – Creating a Hash Based Photo URL	17
Appendix 3 – Including Employees in the Data Feed	18
Appendix 4 – Transferring your Feeds – Additional Items/Guidance	19

UNDERSTANDING HOW WE USE THE DATA FEEDS

The nightly feeds that you provide to Maxient function almost like a telephone directory on the shelf. When your end users need to open a case on a given individual, we look to the most recent feed for initial information about that individual. At that time we copy the content over into our case data structure. This gives us a "snapshot in time". Over time, if aspects of this individual's record change -- new phone numbers, new address, etc. -- we note those changes from your feed and allow your end users to update the case record as needed. If that person is later omitted from your feed because they're no longer enrolled that's not a problem; their information has already been copied into any cases they have for future reference by your conduct officers. Conversely, the average student at a large university who never has a Maxient case will pass through our system in these nightly feeds every day for four years and then simply disappear -- with no information ever having been retained about them in Maxient. This process is perfect for the way Maxient will be used on your campus. Our structure makes life easier for you. Rather than keeping track of who you have or have not sent to us, or what has or hasn't been updated, you simply send us a full set of data nightly and our system will manage the rest.

We recommend that your feed include persons who are currently enrolled, those enrolled the previous term, and those who are already signed up to be enrolled in a future term. This will ensure that needed information is available for your Maxient users even during inter-term periods and summer breaks. If you are looking to include faculty/staff in your data feeds, please refer to Appendix 3, "Including Employees in the Data Feed" for additional guidance.

Below you will find descriptions of the three data feeds, followed by instructions on how to transfer these feeds to us securely. **Please follow these specifications carefully. If something is unclear, please ask for clarification. Unfortunately, we are regularly asked to review sample data feeds that clearly do not follow the guidelines we have set forth. Those circumstances are a waste of both your time and ours.**

FEED #1: DEMOGRAPHIC DATA

Below is a list of fields we'll be expecting in your nightly demographic data feed, in order, and their formatting requirements. While only the unique identifier (SID), name fields, date of birth, and email address are truly required, **the more you provide the more helpful this data set will be to your end users when creating cases.** These fields represent the data most commonly needed by your end users to fulfill their job duties and to provide meaningful statistical reporting on behalf of your institution. Some institutions have additional data they wish to include; please discuss this with your Maxient representative if needed. All data elements should be in plain text unless otherwise noted or arranged with Maxient in advance. An entire data set should be sent each night. If the feed is successful, the previous night's data feed will be purged from the system. If it is not, we'll continue using it and generate an automated error report to you. It is recommended that you include all currently enrolled students, those enrolled the previous term, as well as those scheduled to be enrolled in a future term.

The feed should be one line per student with all fields pipe-delimited. There is no hanging pipe after the final data element. Between entries, a newline will suffice. Within each field, unnecessary leading and trailing spaces should be removed. If a field is empty for a given student, contains invalid information, or will not be transmitted by your institution, it should be included but left empty. An example illustrating this is shown below. Note that in this example, the second student does not have a middle or preferred name.

```
01234567|masmith|Smith|Mary|Ann|MaryAnn|1990-04-15|Female| ...  
55555555|bwilson|Wilson|Brian|||1990-05-25|Male| ...
```

If your institution will be omitting a field entirely (e.g. no GPAs will be sent for any student), please advise Maxient so we'll know to expect that field blank when we first test your feed. Maxient does not support code tables; all values should be transmitted as they are intended to appear for the application's end users. Because fields such as names and addresses will appear in written correspondence, where practical these should be provided in appropriate intercaps (i.e. "Lisa McWilliams" instead of "LISA MCWILLIAMS"). Do not include a header row. For each line, we expect you to account for all of these fields, and to provide them in the following order:

FIELD	FORMATTING REQUIREMENTS AND GUIDANCE	MAX LENGTH
Unique identifier	Format determined by the institution. Student ID number is commonly used (i.e. Banner ID, Colleague ID, PeopleSoft empl ID)	15 characters
Authentication token	Format determined by the institution. Usually corresponds to username or SID. When retrieving correspondence from Maxient, this is used to ensure authentication of the intended recipient.	30 characters
Last name	Free text	50 characters
First name	Free text	50 characters
Middle name	Free text	50 characters
Preferred name	Free text. While it must exist as a field in all record rows, it should only be populated when the Preferred Name differs from the First Name.	50 characters
Date of birth	Format must be YYYY-MM-DD	10 characters
Gender	Must be fully spelled out in intercaps. Valid options are Male, Female, and any others in use on your campus. <i>"M", "F", "MALE", and "FEMALE" are not acceptable.</i>	30 characters
Ethnicity	Valid ethnicity as defined by your campus (i.e. "White, Non-Hispanic"). If multi-variable, delimit using commas or abbreviate.	50 characters
Housing	If student lives on campus, this should be the building name. Otherwise please fill this field with the value "Off Campus".	50 characters
Housing room number	If student lives on campus, provide room number. Otherwise leave this field blank.	10 characters
Local mailing address	Location where student receives official day-to-day university correspondence. Free text.	50 characters
Local city	Leave blank or use "Campus" if local mailing address is on-campus	50 characters
Local state	Free text. Suggestions: leave blank for campus addresses and boxes	2 characters
Local zip	Free text. Suggestions: blank if using campus address, dashes OK	10 characters
Local phone	Free text. Suggestions: parentheses and dashes OK	15 characters
Cell phone	Free text. If available, otherwise leave blank.	15 characters
Permanent address	Location where correspondence intended for the parents/guardian should be sent. Free text.	50 characters
Permanent city	Free text	50 characters
Permanent state	Free text	2 characters
Permanent zip	Free text	10 characters
Permanent country	Free text. Must be blank for USA addresses.	20 characters
Permanent phone	Free text. Parentheses and dashes are OK.	15 characters
Emergency contact	Free text. Spaces, dashes, etc. used to format the information are OK. Usually includes one or more names, relations, and phone numbers. Addresses are generally unnecessary here.	200 characters
Email address	Free text	100 characters
Classification	Valid classifications as defined in your SIS (i.e. Freshman, Not Enrolled, Credit-seeking, etc.)	30 characters
Academic major	Free text. If length is a concern, use abbreviations common on your campus. If you wish to indicate multiple majors (unnecessary), separate the values either a slash ("/") or a comma.	50 characters
Academic advisor	Free text	50 characters
GPA most recent term	Numeric, must be formatted to 3 decimal places (i.e. 3.200, 3.240, and 3.242 are all valid). If no value, leave completely blank.	5 characters incl. decimal
GPA cumulative	Numeric, must be formatted to 3 decimal places (i.e. 3.200, 3.240, and 3.242 are all valid). If no value, leave completely blank.	5 characters incl. decimal
Athletic member	Name of team student is a member of, or "Not Athlete". If this field is not being provided, please put "N/A".	50 characters
Greek member	Name of Greek organization student is a member of, or "Not Greek". If this field is not being provided, please put "N/A".	50 characters
Honors member	Name of honor organization student is a member of, or "Not Honors". If this field is not being provided, please put "N/A".	20 characters

FIELD	FORMATTING REQUIREMENTS AND GUIDANCE	MAX LENGTH
ROTC/Veteran member	Name of ROTC branch student is a member of, or "Not ROTC". Schools may opt to use this as a veteran status indicator instead, with values determined by you. If this field is not being provided, please put "N/A".	20 characters
Honorific	Title preceding an individual's full name (<i>i.e. Mr., Ms., Miss, Dr., Prof., etc.</i>)	20 characters
Pronouns	Subject / object / possessive pronouns / possessive adjective / reflexive pronouns Schools need not provide all five forms, but it is assumed that whatever is provided is in the order listed above. We recommend either a slash ("/") or a comma as the separator. All of the following are valid examples: <i>she</i> <i>she / her / hers</i> <i>he/him</i> <i>they;them;theirs</i> <i>ze / zir / zirs / zir / zimself</i>	30 characters
Last update	The current date. Format must be YYYY-MM-DD.	10 characters

Some campuses may also wish to include additional data elements as part of Feed #1. Maxient can work with you to determine the best approach for those, but when agreed upon, they should be placed as additional fields immediately prior to the "Last update" field. *Each additional field can hold a maximum of 100 characters.*

Schools who will be using Maxient to manage cases involving employees (HR or Title IX) will often include employees in their data feed. See "Appendix 3 – Including Employees in the Data Feed" for additional information.

FEED #2: SCHEDULE DATA

Maxient supports a feed of the current class schedule for each student in the Schedules Data feed, in order to aid in scheduling of meetings, hearings, or in-person delivery of timely correspondence. The format of the schedule can vary by institution, but should generally be free of extraneous information. We do not parse the schedule's content or do any fancy manipulations. Information will be displayed exactly as it appears in the text file, so please be mindful of line length. The best overall appearance will be achieved when individual line lengths do not exceed 80 characters. This includes tabs and other spacing elements. HTML and other markup is not supported. The schedule feed must be provided in a separate plain text file according to the following format:

Line 1: Student unique identifier
Line 2+: Schedule content as you wish it to display
Final line: ***** (10 asterisks)

An example file might appear as follows:

```
01234567
CHEM 111 MWF 10:10-11:00
ECON 102 TTh 9:00-10:15
*****
55555555
FREN 105 MW 8:00-10:00 Prof. Jones Capstone Hall 302
LAWS 303 MWF 11:00-12:15 Prof. Smith Admin Bldg 107
*****
```

Note that the example above shows two different hypothetical layouts. The exact layout is up to you, and perhaps dependent upon your ERP product and how the schedule can best be exported to a flat file. Some schools have found it helpful to format the schedule to match how users have become accustomed to seeing it on the traditional ERP screens. The decision to include items such as room number, section number, class location, instructor name,

and instructor email address is completely up to your institution. Most end users agree this information is valuable to have.

The 10 asterisks are used to indicate the transition from one student's record to another. Schedules should be listed in the file by unique identifier in ascending order, and there should be only one entry per SID. It is permissible for a student to appear in the Demographic Data feed but not in the Schedule Feed. It is also acceptable for the unique identifier to be printed with an empty schedule following it (i.e. if the student is not enrolled in courses for the displayed term).

During the inter-session periods such as late December and July, you should be sending us schedules that reflect the upcoming term. Don't make the mistake of sending an empty file or transmitting no schedules during this period, as that will cause confusion and make things more difficult for your end users.

FEED #3: ID PHOTOS

Maxient can display ID photos for each person present in the Demographic Data feed. We recognize that these photos are often not located in your ERP, but rather in an ancillary system such as CSGold. This will not be a problem, since you will be providing them to us as individual JPEG files irrespective of the system where they are actually stored. You have two options for making these photos accessible in your Maxient system:

- (1) **Preferred method:** Serve the photos from your campus via a parameterized URL. For example, you might tell us all photos can be accessed at [https://www.yourschool.edu/webservices/pictures/\[sid\].jpg](https://www.yourschool.edu/webservices/pictures/[sid].jpg), where [sid] is the student's ID number. We expect the images here to load quickly, so approximate dimensions of 150x150 pixels and 72dpi is ideal. Please do not serve up multi-megabyte high resolution files.

We are frequently asked if this can be restricted to particular IP addresses. Technically, that's not possible because the URL is embedded in pages loaded by end users, so the access will appear to originate from their browser and not Maxient's servers. The URL must be accessible both on and off-campus and not require any type of authentication through your campus identity management system. The best way to accomplish additional security is through the use of a shared secret and hash parameter built into the URL. For general guidance on how you might go about creating a hash-based photo URL service, please refer to the appendix entitled "*Creating a Hash Based Photo URL*".

- (2) **Alternative method:** You may simply send us JPEG files. Any files transferred will be added to the photos on file or will overwrite existing photos of the same name. All images should be placed loose within the `incoming/images/` folder of your Maxient feeds account. They will automatically be resized and moved to production at the same time as your Demographics and Schedule feeds. Most commonly, schools do a one-off bulk upload of photos at the beginning of each term. If you have the ability to send new or updated photos on a nightly basis along with feeds #1 and #2, that's even better. **It is neither appropriate nor permitted to repetitively send all images every day.**

TRANSFERRING YOUR FEEDS TO MAXIENT

Your feeds will be "pushed" to us nightly via Secure FTP (SFTP). In a Windows environment, SFTP using the freely available WinSCP program works well. Once you have developed test versions of the feeds you will be sending, please email support@maxient.com with the subject "*SFTP/Data Feed Setup - **School Name***" and provide the following information:

- (1) **The IP address from where the transfer will originate** - This will facilitate clearance through our firewall. We'll need exact, individual IPs as they appear to the outside world. No ranges, and no NAT/local addresses.
- (2) **A copy of the sending machine's public key** -- This will allow your system to log into our feeds server without a password. The public key should be SSH2 format, either RSA or EdDSA (e.g. Ed25519), and generated without a passphrase. Contrary to its name, a passphrase provides no additional security and prevents you from automating your connection. For more information regarding creating a public key on

Unix/Linux, consult the manual pages for "ssh-keygen". On Windows, we recommend the freely available "puttygen" program.

Please do not encrypt this email or its contents. This is the public half of the key, so there is no security risk whatsoever. Just include it in the body of your email or as a text-based attachment. Once the information listed above has been received, Maxient support will reply with specific information regarding login credentials, file names, folder hierarchies, and the host address. Additional information regarding SFTP command line syntax and GUI automation can be found in the appendix section of this document.

Some campuses firewall their outbound connections. If yours is one, be sure network traffic is permitted to 35.173.72.94 on port 22.

OPTIONAL BACKFEEDS TO YOUR CAMPUS

On occasion, schools find it beneficial to receive feeds of information *from* Maxient. Some examples of this would be when a conduct officer indicates the need to place or remove registration holds, or the assessment of fines to student accounts. Just as you place files on the feeds server for our use, we can automate the placement of files there for you to pick up. Back feeds are not required to make Maxient work, and in fact only a small number of our schools utilize them at all. If this is something that holds particular interest for your school, we recommend waiting until the primary feeds have been completed and the system has gone live on your campus, then reaching out to support@maxient.com to discuss your needs and next steps.

AUTHENTICATION

Maxient strongly recommends authenticating users of our application against your campus identity management system. In addition to making your Maxient system more secure and opening up some additional functionality, this allows you to quickly disable Maxient access in the event an employee is separated from your institution. Keep in mind that even though a user is able to *authenticate*, they still must be *authorized* in Maxient for the particular function they're trying to perform. We do not use attributes from your identity management system to make those decisions.

Whichever method is used, it must be able to authenticate students, faculty, and staff members. For example, if we're doing LDAP binds, we'll need the ability to search your entire tree and not just OU=Students. **Please do not assume that only a subset of these groups will be using Maxient; while it is true that only a small number of your institution's overall population will be "logging in" to the system, anyone at your institution may be interacting with Maxient in a multitude of ways (letter retrieval, authenticating on the incident reporting form, utilizing the People Finder lookup tool, etc). The same is true for CAS and SAML-based methods: you should not be "authorizing" particular users or groups to our application.**

Maxient supports the use of Multi-Factor Authentication (MFA). Refer to "Appendix 1 – Additional Campus Based Authentication Guidance" for details regarding implementing this.

We offer three methods for leveraging your campus authentication systems:

SAML

Our preferred method of authentication is using SAML-based technology such as Shibboleth, Active Directory Federated Services (ADFS), Microsoft Azure, Okta, etc. To make this work we'll need to do a metadata exchange.

We are members of the InCommon Federation and publish metadata as part of their daily updates available for download at <http://md.incommon.org/InCommon/InCommon-metadata.xml>. Alternatively, you may fetch our metadata directly from <https://cm.maxient.com/simplesaml/module.php/saml/sp/metadata.php/maxient-sp>.

If your institution is a member of InCommon, we'll consume your metadata automatically. If you're not part of InCommon, you must provide us with a URL where your metadata lives. We will refresh from that URL hourly, so it must stay live and current.

Your identity provider (IdP) should be configured to release to us a unique and uncommonly recycled identifier (e.g. ePPN, emplID, uid, or such) with which users are familiar. Additionally, we need the user's name as a single attribute (e.g. cn, displayName, etc.). If there are other attributes you normally release to third-party providers, we'll accept those as well -- they won't hurt anything. Once configured on your side and ours, we'll direct you to a test site where we can verify the proper attributes are being released before this authentication method goes live for the production environment.

To set up SAML-based authentication, please email the following to support@maxient.com with the subject "*Campus Based Authentication Setup - **School Name***".

- 1) your entityID as published with InCommon, or the URL of your metadata if only available locally
- 2) which attribute you're releasing to us as the unique and uncommonly recycled identifier

CAS

Native CAS works equally well as SAML. If your server filters or otherwise restricts authentication requests, you must set it to permit all requests coming from addresses under the "cm.maxient.com" domain.

Once configured on your side, please email the following to support@maxient.com with the subject "*Campus Based Authentication Setup - **School Name***".

- 1) your CAS server address and port number
- 2) the URLs for login and ticket validation

LDAP or Active Directory

This is a significantly less preferable option than the preceding two (SAML or CAS), but we'll use it if the others are not available. To accomplish authentication, we attempt a simple bind of your LDAP-based directory over SSL using the ID and password supplied by the user. It is suggested that you create a LDAP service/proxy account for Maxient. To ensure continuity of service, the account should have a non-expiring password. Our application will use this account to locate a user's distinguished name (DN) then attempt to authenticate them.

To get the process started, email the following information to support@maxient.com with the subject "*Campus Based Authentication Setup - **School Name***".

- 1) the bind username and password for our service/proxy account
(password can be provided by phone, if desired)
Example: uid=maxient,ou=services,dc=yourschool,dc=edu
- 2) the directory's address and port number
Example: ldap.yourschool.edu port 636
- 3) the search scope
Example: ou=people,dc=yourschool,dc=edu
- 4) the attribute that corresponds to username
Example: uid=mjones or sAMAccountName=mjones

If your institution permits anonymous binds (uncommon) and all users are located within a single bucket of the directory (e.g. "everyone can be found at cn=(username),ou=school,dc=edu"), a service/proxy account may be unnecessary. In that case, you will only need to provide us with items #2, 3, and 4 above.

Maxient makes no use of any other directory attributes or functions. All authentication attempts will originate from 35.173.227.8 or 34.224.239.82. Please ensure that any necessary firewall rules have been added to permit access to your directory from these IP addresses, and that you have provided us with a monitored email address should we need to inform you of any future IP changes. (Firewall maintenance with IP changes is a big reason we discourage direct LDAP/AD binds in favor of SAML or CAS.)

EMAIL AND SPAM FILTERING

Emails generated by Maxient include incident reports, ping notifications, and correspondence to students, staff, and community members. The very nature of our software means these will frequently involve issues of campus safety and student well-being, and therefore institutions should make every effort to ensure our notices will be delivered to their intended recipients. This includes bypassing filters that might typically be in place for third parties, or language-based filters that could interpret a message containing foul language to be spam. We are not a spammer or a

marketing service; your institution has chosen to use our product to improve its campus operations. The cooperation of your IT department, and specifically your email administrators, will be crucial in the success of this partnership.

All Maxient emails are sent from @maxient.com addresses. Our emails will show a MAIL FROM @sendgrid.maxient.com, and a Header-From @maxient.com, and will pass both SPF and DKIM checks. Maxient does NOT spoof your institution's email addresses.

As of this writing, all Maxient emails will originate from 168.245.32.37. This IP is under our direct control, is used exclusively by Maxient, and will not be the source of any other email.

Below are instructions for optimizing deliverability for each of the common email systems in use on our campuses.

Office 365 / Microsoft Exchange

Step 1: Add our sending IP (listed above) to the IP Allow List using Microsoft's step-by-step guidance ([https://technet.microsoft.com/en-us/library/jj200718\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/jj200718(v=exchg.150).aspx)).

Step 2: For any users that have enabled the Focused Inbox, ensure our messages get there by adding a Transport Rule for all messages coming from the maxient.com domain (<https://support.office.com/en-us/article/Configure-Focused-Inbox-for-everyone-in-your-organization-613a845c-4b71-41de-b331-acdcf5b6625d?ui=en-US&rs=en-US&ad=US>).

G Suite for Education / Gmail

Step 1: Add our sending IP (listed above) to the allowlist in the Google Admin Console using Google's step-by-step instructions (<https://support.google.com/a/answer/60751?hl=en>).

Step 2: Configure Google's spam filter to bypass any messages coming from the maxient.com and sendgrid.maxient.com domains (<https://support.google.com/a/answer/2368132>).

Google's feature set for email administrators is constantly evolving. In early 2019, Google added a series of additional protections, including one that checks the displayed "From:" name on inbound email against names in your organization. While laudable in its intentions, this is highly prone to false positives and particularly troubling for Maxient emails, which will often show a From: address like "Professor Carla Jimenez (via Maxient)". The very measures we take to help the user recognize the email are the measures this Google feature uses to classify our message as a threat. Unfortunately, Google does not exclude third-parties on the allowlist from these warnings when the feature is enabled.

If your institution is choosing to make use of these additional protections, or is seeing continued issues with yellow and red warning banners at the top of Maxient emails, we recommend one additional step:

Step 3: Add our sending IP (listed above) as an Inbound Gateway. To accomplish this, go to Advanced Settings. Then, under General Settings, select your top-level organization (typically your primary domain) on the left. Scroll down to the Inbound Gateway setting located under the Spam section. Hover over the setting and click the Edit button. This will open the Inbound gateway screen.

Safe Links

If inbound email messages are being passed through your EOP system prior to delivery, you may encounter an issue with "Safe Links." Safe Links is a new feature offered by Microsoft Defender for Office 365 that provides URL scanning of inbound email messages in mail flow, and time of click verification of URLs and links in email messages. We've seen a slight uptick in delivery issues related to this new feature, but it's easy to remedy! Here is Microsoft's how-to guide: <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-atp-safe-links-policies?view=o365-worldwide> The links you will want to exempt are:

- *.maxient.com
- *.maxient.com/*
- *.maxient.me/*

FREQUENTLY ASKED QUESTIONS

Does Maxient provide the code to create these data feed extracts?

No, but we'll be happy to put you in touch with technical contacts we may have at other schools using your same ERP. Over the years, we've seen that Maxient clients are happy to offer guidance to their colleagues and share general approaches to constructing good extracts.

We cannot provide all three feeds right now. Will this pose a problem?

The Demographics Feed (feed 1) is required per your Maxient Service Agreement and must be in progress before an on-campus training is scheduled. The Schedules Feed (feed 2) and Photo Feed (feed 3) can be phased in as resources permit. Some schools may be unable to ever provide a photo feed because they don't have photos. That's ok too.

Will we be sending you full demographics and schedules files each day, or just the changes (deltas)?

You are expected to send us full demographics and schedules file each day. We will take care of sorting out any changes on our side automatically. This should make it a lot easier for you! *(With respect to your photo feed, you **will** only be sending updates daily, if you send them daily at all.)*

Does Maxient have a test server that we can send to first?

We don't need one; nothing moves from the feeds server to production until we're certain everything is properly formatted. By having you send your test files to the real feeds server, we can ensure the connection is working as expected. Our staff will review the files and offer feedback on any adjustments that need to be made. Once approved, you let us know by what time we should expect the files to arrive each day, and we'll set our production sweep process accordingly. If you ever want to send test files in the future, and be certain they won't go to production, simply append ".test" to the filename.

What should we name the files? What destination directory should they be placed in?

Specific filenames and directories will be provided by Maxient along with your login instructions for the feeds server. For a refresher on the order of events, see the "Transferring Your Feeds to Maxient" section above.

We'd like to encrypt our demographics/schedules files. Is this possible?

While Maxient does support the encryption of your demographics/schedules files, we do not encourage it. Why? First, we do not believe it is necessary. SFTP is a secure transfer protocol encrypting the data as it moves from your location to ours. The feeds server is properly secured behind a firewall with a default deny rule, and only the individual, key-authenticated accounts for each of our clients are permitted access. The data files only reside on our feeds server from the time you drop them until the scheduled daily sweep, which is often only a few minutes later. Second, troubleshooting issues with encrypted files will be delayed, as not all members of our support staff have the access necessary to manually decrypt the file.

If you still wish to encrypt your file(s), let your Maxient representative know in your Data Feed Ticket and they will provide you with our GPG public key.

We don't store our photos in our student information system. How will we get them to you?

Very few Maxient schools actually keep their ID photos in their student information system. Usually, they are stored in a separate ID card system. You will send them to us via the same feeds server account that's used for the demographics and schedules. This may involve sending them directly from the machine where the photos reside, or perhaps moving them to an intermediate server that handles external file transfers. An even better option: allow us to simply link to them via a URL. For more information, please see the "Feed #3: ID Photos" section above.

Who is the technical contact person for testing the interface and SFTP setup?

Direct all technical inquiries (authentication, feeds, etc.) to support@maxient.com. Different members of our team handle each part of this process, and this ensures the correct person can answer your inquiry in a timely fashion.

Can we expand the feed to include admitted but not yet enrolled students?

Yes. You have considerable latitude in determining exactly who to include in your data feed. Given how the feed is actually utilized in Maxient, it should be focused on the population of people most likely to be involved in a new incident today. These are usually your enrolled students, and perhaps a little more. Some schools will include admitted students, and then drop them from the feed if they have not actually enrolled by some date thereafter (you might be surprised at how many admitted students find their way to trouble during their orientation visit). Other schools will keep students in the feed for a semester or so even after they have withdrawn from the institution. Reading this, you might be tempted to include individuals who have long since left the institution, but that would be a bad idea as the information you have for them (home address, phone number, etc.) is likely outdated. Plus, unnecessary bloat of the data feed can impact system performance. Keep in mind that cases can still be opened in Maxient even for individuals not present in the feed. The feed serves only to make case creation easier and your data more accurate; it in no way limits who can have records in Maxient.

Should we (or can we) include faculty and staff in the data feed?

Yes, you certainly can include them. Some fields would naturally be blank for faculty and staff, and these should be fairly obvious. Whether or not you should include these folks is determined by whether your end users will be opening cases *about* them. If Maxient will be used for employee behavioral intervention efforts, or as part of your HR office, then the answer is "yes". Typically, the "Classification" field is the place where schools will identify someone as an "Employee" (versus the more obvious classification values for students). Refer to the appendix entitled *"Including Employees in the Data Feed"* for additional guidance.

We need to provide a "Preferred Name" for some students. How do we do that?

Maxient supports a preferred name/nickname field. In the standard data feed file order, the "nickname" (preferred name) field falls between Middle Name and Date of Birth fields. While it must exist as a field in all record rows, it should only be populated when the Preferred Name differs from the First Name.

The preferred name is a new Maxient standard data feed field as of 2020. If you do not currently include the preferred name field but wish to do so, please email support@maxient.com, and we will assist you. If you are not currently sending this field, please do NOT update your field order without notifying Maxient.

We have some additional data elements we'd like to send. Where can we put those?

Additional data elements must be cleared with Maxient first. Please speak with the Maxient staff member who provided you this document and explain to them what you'd like to include. They will advise the best location and appropriate formatting suggestions.

How can I determine my publicly-facing IP address?

If you will be sending files from a Windows environment, point the server's web browser to www.whatismyip.com. If you will be sending from Unix or Linux, paste the following onto the server's command line and press Enter:

```
curl -s http://checkip.dyndns.org | sed 's/[a-zA-Z/<> :]/g'
```

My IP address is 192.168.x.x, 172.16.x.x, 10.x.x.x, or something very similar.

No, it's not. IPs in those ranges are considered local, private, or NATed addresses. They are usable only within your campus network. If the steps provided in the question immediately above result in an IP like this, contact your network administrator and ask for assistance. Tell him/her that we need to know how your IP address appears to the outside world.

When connecting to the Maxient feeds server, we're getting a "Connection timed out" error.

This indicates your connection is either firewalled outbound from your campus (less likely), or is coming from a different IP address than the one you provided to us (more likely). Check with your network administrator to ensure that outbound SFTP connections on port 22 are permitted from your machine. Then double check the IP you provided using the instructions above.

When connecting to your feeds server, we're being prompted to enter a password.

This means that your SFTP client is not "seeing" your SSH private key, so it thinks you're using password-based authentication and is prompting you accordingly. Check to ensure that your command-line or SFTP client has the proper paths to the location of your private key.

We've never sent data feeds out of our institution before. What programs do you recommend for SFTP from Windows or from Unix/Linux?

On Windows, most of our clients use WinSCP with great success. The program is available for free from www.winscp.net, and can support automated transfers and scheduling via the Windows Task Scheduler. On Unix and Linux, we recommend the command-line program "sftp", which is typically built-in to the operating system.

Can you describe Maxient's hosted infrastructure?

Maxient's operations are housed entirely within Amazon Web Services (AWS), and specifically the US-East-1 (Northern Virginia) and US-West-2 (Oregon) regions. Our application is architected as a multi-tenant environment, served by a fleet of EC2 instances running Amazon Linux and the Apache web server, and backed by a MySQL database running on Amazon's Relational Database Service (RDS). These resources are contained within a Virtual Private Cloud (VPC) and are accessible only via HTTPS. Additionally, we operate a publicly-addressable SFTP site in AWS for the purpose of passing data feeds between the Maxient environment and our client institutions. Access to this site is restricted to pre-authorized source IP addresses and only supports the SFTP protocol.

To enhance the redundancy and performance of its service, Maxient makes use of several other AWS-based technologies including DynamoDB, S3, and Route 53.

More Information regarding Amazon Web Services' security posture, audits, and certifications can be found at <https://aws.amazon.com/security/>.

Can you describe the steps taken to ensure the security of data both in transit and at rest?

The safety and security of your data is fundamental to our business. Beyond the physical security at our datacenters, we take several other measures to improve security. Data feeds between your institution and our servers are sent via SFTP and are therefore encrypted in transit. Sensitive data elements at rest are encrypted with a variety of methods, most commonly AES-256 and GnuPG on files. For institutions that store authentication credentials with us locally, a currently accepted strong cryptographic algorithm such as Blowfish is used. As a policy we encourage schools to allow us to authenticate users against their authoritative directory service rather than using Maxient-based password stores, and the majority see the value in doing so. All end users interact with the system through the web over HTTPS 256-bit AES-encrypted TLS. We operate separate production and development environments to ensure integrity of the live application and its data. Maxient servers are protected by a hardware firewall, network segmentation, and a proprietary intrusion prevention system. Your data is stored only on our servers, not on laptops or other company-owned devices that could be subject to loss or theft. Our employees are bound by the confidentiality provisions in the Maxient Service Agreement, which may also incorporate confidentiality agreements your institution traditionally requires of third-party contractors or employees. All actions within Maxient are logged and audited. We actively monitor usage by developing a fingerprint for each user. Usage that falls outside of the established pattern is flagged for our review and may result in automatic account locking. As part of your contract with Maxient, all of your data will automatically be backed up nightly, encrypted using asymmetric key pairs, and transmitted over an encrypted connection to our secondary AWS data store in Oregon. These offsite backups are retained by Maxient on a rolling cycle for the most recent month (approximately 30 days). Should it become necessary, due to breach or otherwise, recovery can be accomplished with a minimal amount of downtime (average 30 minutes). Several other security measures, both minor and major, are in place which we do not disclose publicly.

What is Maxient's policy for responding to a security breach?

Should any Maxient employee or agent become aware of a potential data compromise, they are obligated to notify their supervisor immediately. An investigation will commence to identify the scope of the breach, along with immediate notification to any potentially affected customers. Maxient will remain in constant communication with all affected customers, advising of the results of our investigation and what corrective actions are being taken. At the conclusion of the investigation, Maxient will furnish a full report along with an action plan to prevent future occurrences. Additional specifics regarding our response and communication with customers may be found in the Maxient Service Agreement.

Can you describe Maxient's business continuity and disaster recovery plans?

Maxient has a comprehensive business continuity plan that includes the archiving of critical corporate information and application source code on physical media at a secure off-site location, as well as in the cloud. Multiple members of our management team have access to, and the authority to use, these contents in the event of a disaster impacting business operations or loss of critical personnel.

Specific pathways in our disaster recovery plan (DRP) are largely dependent upon the scope of the disaster and vary for different components of the application. For example, in the event of a hardware-related outage, our systems

©Copyright MAXIENT 2022. All rights reserved.

Contains confidential information proprietary to MAXIENT – not to be disclosed to third parties without MAXIENT's prior written permission.

have been architected to redirect traffic around failing instances and to leverage AWS auto-recovery functionality. Our distributed and redundant system architecture helps to mitigate the risk of a single point of failure, or even failure at the availability zone level. Should a full-scale disaster cause a prolonged disruption to our operations (e.g. natural disaster impacting the entire United States, massive DNS outage, etc.), institutions would need to maintain records locally until such time as Maxient's systems are back online and available for data entry. Our primary backup methods allow for a Recovery Point Objective of 24 hours, but as we leverage more of the features AWS offers, we anticipate being able to drop the RPO to perhaps as low as 1 hour. Because Maxient is rarely a mission-critical application for most campuses, we have not formally defined a specific Recovery Time Objective. Our DRP is reviewed continually and tested with dry runs looking at 2-3 plausible scenarios on an annual basis.

Who owns our data? And what happens if Maxient goes out of business or we vacate our contract?

Maxient's Service Agreement makes it clear that you – the college or university – retain complete ownership and control over your data at all times. This is consistent with the requirements of prominent privacy laws, including but not limited to FERPA and GDPR. Maxient will never sell your data or release it to third parties without your permission. Should you decide not to renew your Maxient contract, all data will be exported back to you in a flat-file format suitable for import into another database or commercial product. Additionally, any documents saved within the Maxient system will be provided via SFTP in a folder structure that matches the case numbering system. Maxient will eliminate all copies of your data from our servers and overwrite to industry standards to ensure the data is not recoverable.

Can an institution using Maxient be FERPA compliant?

Yes. The Family Educational Rights and Privacy Act (FERPA) is a US federal statute that applies, in the context of higher education, to any college or university receiving any federal funds. Among other things, FERPA provides limits on the disclosure of student "education records." Maxient is a third party permitted to receive and provide services to institutions related to those education records in accordance with FERPA's governing regulations (See, 34 C.F.R. § 99.31(a)(1)(i)(B)). Specifically, to comply with FERPA, Maxient must (1) perform a service or function for which the institution would otherwise use employees (e.g., managing student conduct records); (2) do so under the direct control of the institution with respect to the use and maintenance of education records; and (3) abide by the requirements of FERPA's governing regulations on the use and re-disclosure of personally identifiable information from education records. Maxient does this for all of its clients and guarantees it in writing in all of its service agreements.

Nothing about the intended use of Maxient's software will cause an institution to run afoul of FERPA. However, it is important to remember that complete compliance with the law cannot be guaranteed by simply using a particular software, Maxient or otherwise. Rather, being FERPA compliant is ultimately incumbent upon the institution, and it is measured by that institution's policies and its adherence to those policies.

What about HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) is a comprehensive federal health care law that among many other things establishes limits and conditions on the disclosure of "protected health information" (PHI). HIPAA is essentially inapplicable to a service like Maxient's. While some colleges and universities using Maxient may themselves be covered entities under HIPAA, and some may even store information in their Maxient systems that could constitute student PHI, the records stored in Maxient nevertheless remain "education records" under FERPA. Per the joint guidance of the Department of Health and Human Services and the Department of Education, where both HIPAA and FERPA may apply, FERPA governs. That joint guidance may be viewed at <https://studentprivacy.ed.gov/resources/joint-guidance-application-ferpa-and-hipaa-student-health-records>.

What about GLBA, FACTA, or the Red Flags Rule?

The Gramm-Leach-Bliley Act (GLBA) and Fair and Accurate Credit Transactions Act (FACTA) are federal laws, and the Federal Trade Commission's "Red Flags Rules" are federal regulations, that among other things strengthen privacy protections for consumers, which includes students at institutions of higher education. Maxient, however, is neither a "financial institution" nor a "creditor," within the meaning of those laws, and its software does not utilize or contain personal financial information, such as bank account or credit card numbers. While institutions served by Maxient may well need to comply with GLBA, FACTA, and the Red Flags Rule, their use of Maxient's software is unrelated.

What about CCPA?

The California Consumer Privacy Act (CCPA), which went into effect on January 1, 2020, is a state law that offers added privacy protections and rights to Californians through its application to businesses engaged there, regardless

of the covered business's location. It does not apply to non-profit entities, which constitute the near entirety of Maxient's clientele of colleges and universities, nor does it actually apply to Maxient because Maxient does not meet any of CCPA's thresholds for the definition of a covered business (See Cal. Civil Code § 1798.140(c)). Specifically, Maxient neither purchases nor sells consumer information. Notwithstanding, any discussion contemplating the spirit of CCPA and the work between Maxient and its clientele is best informed by two key facts: (1) There are sufficient guarantees in all Maxient service agreements about the limited purposes for which any confidential information is used, and (2) Rights of access to applicable personal information via the controlling institution are well established under FERPA due to the record's context as an education record within the meaning of that law.

What about the GDPR?

GDPR stands for "General Data Protection Regulation," the informal title of Regulation (EU) 2016/679, which is a privacy law established by the European Union ("E.U."), that can be applicable even to organizations outside of Europe, including colleges and universities in North America. For the majority of Maxient's clients, GDPR will have little to no applicability to their use of their Maxient systems; but for others, it may. Regardless, Maxient can and does establish stipulations in its standard service agreements that are consistent with Article 28 of GDPR's obligations of processors (what GDPR calls third party entities, like Maxient, that handle data on behalf of "controllers," i.e., colleges and universities in this context). Moreover, some key truths of every working relationship between Maxient and its clients that tend to alleviate GDPR concerns are as follows:

- The college or university always exercises complete control over the data it stores in a Maxient system.
- Maxient never shares any institution's data with any third parties, or otherwise uses the data for any purpose, other than that which is specified under the service agreement.
- In the event of a termination of services for any reason, Maxient ensures that the institution takes full possession of the data and Maxient does not retain any copies whatsoever.
- All data in a Maxient system is encrypted both in transit and at rest.
- All data in a Maxient system is backed up on a rolling, thirty-day basis to a geographically separate server site to better ensure the continuity and availability of the data in the event of catastrophe. See, GDPR, Art. 32(1)(c).
- In the event of a data breach, Maxient would notify any impacted institution as immediately as is practicable, but in no event later than 24 hours following discovery.

Lastly, if applicable to your institution (located in the E.U. or operating a campus within the E.U.), Maxient is willing to supplement your Maxient service agreement with a copy of the Standard Contractual Clauses, completed and provided by your institution, so long as they do not substantively deviate from those published by the European Commission (see here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en).

Has Maxient ever experienced a security breach or been the subject of a legal action?

No.

What is Maxient's insurance coverage?

Maxient carries insurance well in excess of any reasonably foreseeable costs that could arise from its services. Specifically, Maxient maintains \$4,000,000 in General Liability, as well as an additional \$2,000,000 in Errors & Omissions (including coverages for data breach and privacy notification costs) and \$1,000,000 umbrella coverage. A certificate evincing these coverages currently in effect can be provided upon request.

Can Maxient integrate with our campus directory/authentication service?

Yes. Maxient strongly recommends authenticating users of our application against your campus identity management infrastructure. In addition to making your system more secure, this allows you to quickly disable access in the event an employee is separated from your institution. Our preferred method is with SAML, including Shibboleth or ADFS, or with CAS. Direct LDAP or AD binds are also an option, albeit less preferentially. Please refer to the section above titled "Authentication" for more information.

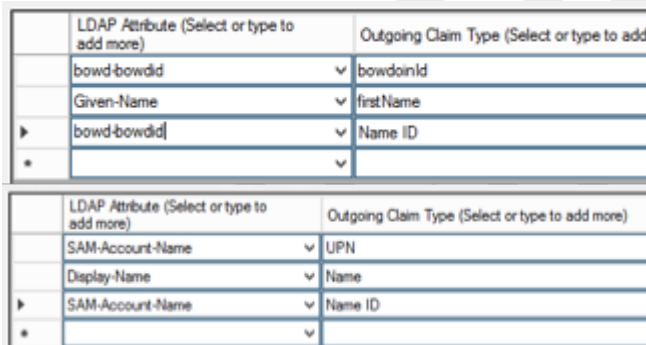
So is there a prize for having read this whole thing?

No, but you certainly have our appreciation and respect! Those who do so usually report this implementation to be one of the easier and more organized software-as-a-service projects with which they've been involved!

CONFIDENTIAL

Appendix 1 – Additional Campus Based Authentication Guidance

1. Metadata must be provided by URL – we cannot accept standalone XML files
2. **Multi-Factor Authentication (MFA):** Maxient supports the use of Multi-Factor Authentication. To establish the MFA, we will need the multi-factor context, also referred to as AuthnContextClassRef. One example common value for this field is "https://refeds.org/profile/mfa".
3. Some SAML Software pulls URLs and endpoints directly from Maxient's metadata while other software requires you to enter the values manually.
 - Maxient Metadata URL:
 - <https://cm.maxient.com/simplesaml/module.php/saml/sp/metadata.php/maxient-sp>
 - Maxient ACS URL:
 - <https://cm.maxient.com/simplesaml/module.php/saml/sp/saml2-acs.php/maxient-sp>
4. **Azure:** Maxient is published in the Azure Marketplace – Search for 'Maxient Conduct Manager Software' and continue the setup. The URLs and Endpoints should be loaded for you.
 - You can view a setup tutorial here: <https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/maxient-conduct-manager-software-tutorial>
 - Before you complete your setup, **please ensure that user assignment is disabled**. The setting is called "User Assignment Required," and should be toggled to "No."
5. **ADFS:** ADFS works well, but 'Name ID' must be included in your outgoing claim. We recommend releasing the "Uncommonly Recycled" attribute that Maxient will authorize users against twice. Once as 'Name ID' and the second with a name that makes sense for your institution. See two screen shots below:



The image contains two screenshots of a configuration interface, likely for SAML. Each screenshot shows a table with two columns: 'LDAP Attribute (Select or type to add more)' and 'Outgoing Claim Type (Select or type to add more)'. The first screenshot shows 'bowd-bowdid' mapped to 'bowdoid' and 'Given-Name' mapped to 'firstName'. The second screenshot shows 'SAM-Account-Name' mapped to 'UPN' and 'Display-Name' mapped to 'Name'.

LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
bowd-bowdid	bowdoid
Given-Name	firstName
bowd-bowdid	Name ID

LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
SAM-Account-Name	UPN
Display-Name	Name
SAM-Account-Name	Name ID

In the example screen shots above, you will see one school is releasing 'bowd-bowdid' and another is releasing 'SAM-Account-Name'. The name of this attribute will vary from school to school, so you should be choosing the correct attribute for your institution. In your Outgoing Claim, you will choose 'Name ID' for one of the two attributes you have selected in the LDAP Attribute column. The other attribute can be named whatever makes sense for your institution.

6. **OKTA:** Values typically used in OKTA setups are as follows:
 - Single Sign on URL:
 - <https://cm.maxient.com/simplesaml/module.php/saml/sp/saml2-acs.php/maxient-sp>
 - Recipient URL:
 - <https://cm.maxient.com/simplesaml/module.php/saml/sp/saml2-acs.php/maxient-sp>
 - Destination URL:
 - <https://cm.maxient.com/simplesaml/module.php/saml/sp/saml2-acs.php/maxient-sp>
 - Audience Restriction:
 - <https://cm.maxient.com/simplesaml/module.php/saml/sp/metadata.php/maxient-sp>

7. **OneLogin:** Values typically used in OneLogin setups are as follows:

- Audience (EntityID):
 - <https://cm.maxient.com/simplesaml/module.php/saml/sp/metadata.php/maxient-sp>
- Recipient:
 - <https://cm.maxient.com/simplesaml/module.php/saml/sp/saml2-accs.php/maxient-sp>
- ACS (Consumer) URL Validator:
 - [^https://cm.maxient.com/simplesaml/module.php/saml/sp/saml2-accs.php/maxient-sp](https://cm.maxient.com/simplesaml/module.php/saml/sp/saml2-accs.php/maxient-sp)
- ACS (Consumer) URL:
 - <https://cm.maxient.com/simplesaml/module.php/saml/sp/saml2-accs.php/maxient-sp>
- Single Logout URL:
 - <https://cm.maxient.com/simplesaml/module.php/saml/sp/saml2-logout.php/maxient-sp>

Appendix 2 – Creating a Hash Based Photo URL

On our side, we're able to specify a URL through which any given student photo can be located at a school. The simplest example would be something like this:

```
https://photos.school.edu/images/1234567.jpg
```

 where "1234567" is the student's ID.

On our side, we'd plug that in like this:

```
https://photos.school.edu/images/{SID}.jpg
```

and our application dynamically takes care of the rest.

The problem with that approach is that, in theory, anyone with that URL could also access the photos. There needs to be something about the URL that guarantees only we can use it, and that when it's used, you can verify that it's really us. The most common way to accomplish that is with a shared secret that becomes part of the URL. This is the basis for most modern-day web services (APIs, etc.). So, let's say we agree on the shared secret phrase being "Ice cream is great on a hot day". Now, we create an MD5-based hash using that phrase and the SID. In most programming languages there is a built-in function for accomplishing this. I write PHP, so in PHP the code looks as follows:

```
$hash = md5("Ice cream is great on a hot day".{SID});
```

This reflects the concatenation of the phrase and the SID, then run through the MD5 algorithm. That will result in `$hash` being equal to something like this: `sdSSMXL2dsxzs873woqjlnklvnasljdjfi8323xNND2`.

So on our side, we'd dynamically build the URL every time we go to access a photo. Rather than the original insecure URL I showed at the top of this message, we'd now send you something like this:

```
https://photos.school.edu/images/getphoto.php&sid=1234567&hash=sdSSMXL2dsxzs873woqjlnklvnasljdjfi8323xNND2
```

On your end, the "getphoto.php" script would read the two parameters, the SID and the hash. You'd take the SID we provided, and you'd calculate the hash on your side by combining it with the secret phrase. If you come back with the same value that we provided as the hash, then you know it's a legitimate request because that means we knew the shared secret. If the hashes don't match, you don't display the photo because the request cannot be trusted.

To make this more secure, you can add a third parameter which specifies the time of the request using a Unix timestamp. By requiring that the timestamp fall within certain bounds of the current time on your side (e.g. +/- 10 minutes of your server's clock), you can effectively eliminate the possibility of someone using a replay attack (an old link tried again hours or days later) or brute forcing attempts to guess the secret phrase. For example:

```
https://photos.school.edu/images/getphoto.php?sid=1234567&time=1409885539&hash=sdSSMXL2dsxzs873woqjlnklvnasljdjfi8323xNND2
```

where the hash = `md5("Ice cream is great on a hot day" + SID + time)`

Lastly, you could add a fourth parameter ... something like "service" ... to indicate which service provider (e.g. Maxient) the request is coming from. With this, the script you've created becomes robust and scales nicely. This would allow you to have different secret phrases for each company you work with, so if a relationship terminated or a phrase became compromised, you could change it without disruption to your other services. The phrases could be set up as a simple array in your script, so that when a URL comes in, you look at the "service" parameter to decide which secret phrase to use when calculating the hash.

The photo you serve up still needs to be of a reasonable byte size (40kb or less) and reasonable dimensions (approximately 150px on the long side).

Appendix 3 – Including Employees in the Data Feed

Schools who will be using Maxient to manage cases involving employees (HR or Title IX) will often include employees in their data feed. **Schools must include students and employees in a single demographics file.** Student entries in the file are already clearly outlined above. Here's how those fields translate for employees:

- All LOCAL address and phone-related fields are considered relative to their work on the campus (e.g. Jones Tower 302).
- All PERMANENT address and phone-related fields are considered to be their place of residence.
- CLASSIFICATION is used to denote something basic like "Employee", or at your option, a more specific category of employment (e.g. "Admin Spec II")
- ACADEMIC MAJOR is their department
- ACADEMIC ADVISOR is their supervisor
- GPAs are blank and all MEMBERSHIP fields are "N/A" or "Not _____", as appropriate based upon what you are providing for students.

Employees usually do not appear in the schedule feed file. You are welcome to provide ID photos for them in the same manner you provide students to Maxient.

Appendix 4 – Transferring your Feeds – Additional Items/Guidance

IP ADDRESSES

In keeping with good, secure design, this server is firewalled and accessible only by specifically authorized IP addresses. You must provide us with the IP address(es) from which you will be connecting, as they appear to the outside world. Internal IPs (e.g. 192.168.x.x, 10.1.x.x, etc.) are not valid since they apply only within your local network, and broad IP ranges are not acceptable either for security reasons. If your IP address changes, you'll need to ask your networking staff to make it static. Your IP address can be easily determined as follows:

Windows: Go to www.whatismyip.com from the machine you will be using to do the transfers.

Unix/Linux: Paste the following onto your server's command line and press Enter:

```
curl -s http://checkip.dyndns.org | sed 's/[a-zA-Z/<> :]/g'
```

PASSWORDS VS. SSH KEYS

To maintain the most reliable and secure ability for you to connect to our feeds server, Maxient strongly prefers the use of SSH keys in lieu of passwords. The use of a password will only be approved if the sending server does not support the use of an SSH key (this is rare). The key you create should be SSH-2 RSA or EdDSA, and without a passphrase.

Windows: Use the freely available program "puttygen". More information and detailed instructions can be found here: http://winscp.net/eng/docs/ui_puttygen

Unix/Linux: Use the command-line tool, `ssh-keygen` .

CONNECTING FROM WINDOWS (WINSCP)

If you have not already done so, download a copy of WinSCP by visiting www.winscp.com .

After we've replied back with account credentials, the next step is to start WinSCP and add the settings for connecting to Maxient. WinSCP refers to this as a session, and you can usually add a new one immediately upon loading the program. You'll add the hostname, username, and select the location of your private key file. Leave the password field blank. For the connection type, choose "SFTP". Save these settings, then connect and make sure that you are able to get logged into our server. On the first attempt, you may be prompted about a "Host Key" -- either that it wasn't recognized, or perhaps that it needs to be added. Simply answer with the affirmative (Yes, OK, etc.) and the connection should proceed. This establishes a trust relationship so that your computer recognizes our server in the future. You'll know you're logged in and at the correct place when the right half of the screen shows several directories and one of them is "incoming". The "incoming" directory is where you'll be placing your files with a simple drag and drop.

If you're having trouble at this point, the WinSCP documentation is a great place to start. Available at <http://winscp.net/eng/docs/start>, there's a helpful table of contents that should allow you to hone in on the particular area of your troubles and get it resolved.

CONNECTING FROM UNIX/LINUX

A simple one-line command will usually accomplish the task of connecting to our server, dropping the file, and logging out:

```
sftp -oIdentityFile=[private key path] [username]@feeds.maxient.com:incoming/ <<<  
$'put [local_file_path]'
```

A complete example might look as follows (note that this is broken across two lines purely due to length):

```
sftp -oIdentityFile=/usr/banjobs/id_rsa school@feeds.maxient.com:incoming/ <<<
$'put SCHOOL_DEMOGRAPHICS_DATA.txt'
```

AUTOMATING THE FILE TRANSFER UNDER WINDOWS (WINSCP)

Once you've established that you can successfully connect to our server manually, we recommend creating a script that will allow you to automate the transfer to run on a daily basis with no manual intervention. Begin by creating a new plain text file. For the sake of our example, we'll call it `maxconnect.txt` and give it the following contents:

```
option batch on
open school@feeds.maxient.com
cd incoming
option confirm off
option transfer ascii
put C:\MAXIENT_FEEDS\SCHOOL_DEMOGRAPHICS_DATA.txt close
exit
```

In this example, "school" would be replaced by the appropriate username and filenames provided to you by Maxient. This brief script establishes an SFTP connection, changes to the proper directory, drops a single file, and then disconnects.

More information on automation with WinSCP may be found at <http://winscp.net/eng/docs/scripting> . Once you have your script working, the Windows Task Scheduler will allow you to set the days and times that it will run. The command it needs to run is the following:

```
winscp.exe /console /script=maxconnect.txt /privatekey=privkeyfile.ppk
```

Note that we have assumed your private key file is named `privkeyfile.ppk` and located in the same directory as the script. If that's not the case, you may need to modify the line above to include the absolute path to each file, like this:

```
winscp.exe /console /script=C:\MAXIENT\maxconnect.txt
/privatekey=C:\MAXIENT\privkeyfile.ppk
```

We've had some reports that the "winscp.exe" file does not run properly under 64-bit Windows pseudo-DOS environment. If problems persist and you're running from that command line, try "winscp.com" instead.

AUTOMATING THE FILE TRANSFER UNDER UNIX/LINUX

Once you've established that you can successfully connect to our server manually, the `cron` utility should be used to schedule the transfer on a nightly basis.