Overview of setting up SIP2 (Self Check) for Voyager

- **Product:** Voyager
- **Relevant for Installation Type:** Multi-Tenant Direct, Dedicated-Direct, Local, TotalCare

Question

Overview of the steps required to setup SIP2 (Self Check) for Voyager.

Note

Self Check is not part of the standard Voyager implementation. See: How do we activate Self Check (SIP2) for Voyager?

Answer

Equipment and/or resources use the SIP2 protocol to communicate with Voyager. These products include "Self Check machines" (e.g., "3M") which are used for self-service circulation. The products also include some hosted eBooks services (e.g., OverDrive) for authentication, as well as other products that rely on the SIP2 protocol such as book sorters. Recently functionality has been extended to smart devices. Note that Ex Libris does *not* maintain a list of those products.

Voyager includes a subset of the formal 3M Standard Interchange Protocol 2.00 (SIP2) to provide authentication for and communication with self-check machines[1]. Ex Libris develops and defines this subset. While Voyager SIP2 does not include or reference all elements of 3M's protocol, Voyager libraries can use SIP2 effectively for transactions involving self-check hardware and/or patron authentication for electronic resources.

Initial Setup

Regardless of the application for which you need SIP2, you will need to perform the following setup in the Voyager System Administration client. You will need SysAdmin permissions for Security, System Wide Configuration, and Circulation Policy Groups to complete all steps. Please refer to the Interface to Self Check Modules Using 3M SIP User's Guide, Chapter 2 ("Setting Up SIP Self Check) for detailed instructions on the following steps, which are meant to provide a helpful overview.

This article is not a substitute for reading the User's Guide.

1. Create a unique SIP2 location in Voyager

Voyager requires that SIP2 applications log in to a designated Happening Location to perform transactions. Support recommends that you create a location that is different from your standard circulation happening locations, so that reports will show SIP2 transactions distinct from regular circulation, and so that you can troubleshoot any access problems more effectively.

Choose a location code that you can easily distinguish from shelving locations, as well as other happening locations. (For instance, start the location code with a “Z” or include “SIP2” in the location code.)

Remember to add the new location to the appropriate "MASTER" Security Profiles before you continue (see Add a New Location to Voyager for detailed instructions on adding a new Location).

2. Create a SIP2 operator

Create a unique username and password that your SIP2 application will use. You will share this operator credential with the application or hardware vendor, so it should not be the same as any existing account.

3. Create a SIP2 circulation security profile

A SIP2 operator’s privileges do not need to be extensive, since this operator will not use a regular Voyager client. The self check operator also will not require access to any other happening or shelving location than the one you established for your SIP2 application in Step 1.

- Create the security profile with a unique name.
- Add the self-check operator on the Operators tab.
- Add the self-check happening location on the Locations tab.
- On the Profiles tab, keep “Charge/Renew,” “Mask Patron Social Security Number,” and “View-Only Patron Records” checked; leave other settings unchecked.
- Do not add the self-check happening location to unnecessary Security Profiles to prevent *normal* desk operators from logging into it.

4. Create a new circulation policy group, and add the SIP2 location

To establish the SIP2 location as a happening location, you must add it to a Circulation Policy Group. Support recommends that you create a separate policy group for SIP2 applications. Doing so enables the library to test and implement applications without impacting existing circulation policies.

A SIP2 policy group may be created with minimal settings. If a SIP2 location will be used only for SIP2 authentication, you do not need to create any matrix entries beyond the “all/all” entry. This same location may be used to charge items without creating matrix entries, as Voyager will use the policy group for the location of the *item* being charged.

- Create a policy group with a unique name.
- Add at least one calendar on the Calendars tab.
- Add the SIP2 location on the locations tab.
- Edit the SIP2 location, and check the Circulation Location box to make it a valid happening location. Set the Shelving Interval, In Transit Interval, and Hold Life to be the same as your main policy group.
- Add or edit the “all/all” entry on the Matrix tab in order to establish default circulation settings for the policy group. You may leave all settings unchecked and blank if you will only be using the policy group for authentication.
- Edit the settings on the Policies tab to be the same as your main policy group.

Optionally, you may choose to apply similar blocking conditions to SIP2 activity as you use at your circulation desk. If so, edit the patron groups tab to reflect the limits you want to set. If a patron has exceeded any of these limits, that patron will be blocked from authentication and circulation activities over SIP2.

5. Test

Once you have defined the SIP2 location, operator and policy settings you can begin to work with the application/hardware vendor to test connectivity, communications and functionality.

Note that firewall rules may need to be modified (Voyager Self-Check runs on port xx31 by default).

Try logging into the Circulation Client with the credentials created in Step 2. You should be able to select the happening location created in Step 1.

The vendor will require the following information:

- Your Voyager server details/address.
- Username: the SIP2 operator login you created in step 2.
- Self-Check Password: the SIP2 operator password you created in step 2.
- Self-Check Location Code: the SIP2 location code (not the location name) you created in step 1.
- Port: XX31 where XX are the first two digits your library uses in the Voyager.INI port numbers on your PC.

You may need to communicate to the vendor that Voyager uses a modified version of the 3M SIP 2.00 protocol: one that does not use every message or feature. Voyager also includes some proprietary elements, which you may review in the "Setting up SIP Self Check" chapter of the Interface to Self Modules of 3M SIP Documentation Some of these include:

- Voyager expects communication over a socket connection type.
- Messages must be terminated with return characters only. Voyager will not respond correctly if vendor system messages contain newline characters.
- Voyager does not use checksums in messages. Turn off checksum and error checking on the Self-Check machine.
- Voyager does not support PINs.
- For the login message (msg93), Voyager expects the self-check operator username, operator password, and the self-check location that you defined above.
- For the patron information response message (msg 64), Voyager will return the patron group code in field “PT” at the end of the message; this field is proprietary to Voyager, so you will need to inform your vendor of its location.
- When a patron is not eligible to borrow an item, the patron information response message (msg 64) will include the value “N” in field “CQ.” Some vendor systems will interpret this response as “invalid PIN” or “invalid password.”

Note

No two SIP2 applications or SIP2 vendors are alike. Each new application/vendor may have unique requirements as to how the protocol should be configured and how it will perform.

Additional Information

[1]Note that the Ex Libris SIP2 server for Voyager is limited in functionality. Ex Libris does not implement the full protocol standard, only the functionality needed to interface with SelfCheck (SIP2). The SIP2 protocol is implemented in a client-server fashion. The SIP2 application programming interface (API) is standardized and (to the degree that it is implemented in the software) the same for any ILS. However, on either side of that protocol/API are client and server applications. The SIP2 *server* application (the "extension module" that is licensed separately from the Voyager software) is ILS-specific, while the SIP2 *client* application is ILS-agnostic. That means that a SIP2 server designed to work for one ILS, won't work for any

other ILSs. It is *ILS specific*.

See also:

- Add a New Location to Voyager
- Setup for communication with Voyager Self Check module
- Voyager Self Check module basic protocol reference
- Voyager Self Check test perl script
- Are certain self-check vendors recommended for use with Voyager?
- Interface to Self Check Modules Using 3M SIP - March 2014.pdf?revision=1
- "3M Standard Interchange Protocol" Version 2.

- **Article last edited:** 20-Jul-2020