I used the self check product documentation to begin setting up the machine:

<https://knowledge.exlibrisgroup.com/Alma/Product_Documentation/Alma_Online_Help_%28English%29/Integrations_with_External_Systems/040Fulfillment/060Self-Check_Machines>

1. On the General Configuration page (Administration > General Configuration > Configuration Menu), click Integration Profiles under External Systems. The Integration Profile List page opens.
2. Click Add Integration Profile. The first page of the integration profile wizard opens
3. Perform the following actions on this page:
 In the Code and Name fields, enter a code and name (respectively) for the profile you are defining. **Note: I used all lower case and no spaces for my selfcheck code. It’s best to use this format for all codes in Alma. Since we only have one circ desk that uses the self check, it didn’t matter what I named it. I would suggest coming up with a naming scheme if you have more that one circ desk that uses a self check.**
4. From the Integration type drop-down list, select Self-check.
 In the System (for Ex Libris’ informational purposes) field, indicate the type of self-check system with which you are integrating. Note that this is mandatory.
 Optionally, in the Description field, enter a description of the integration you are configuring
5. Click Next. The second page of the wizard opens.
 Under General Information, perform the following actions:
 In the SC Identifier field, enter any string. **Note: at first I was a little confused by this as I already have a name for the self check, but apparently Alma wants two names (one for the external system and one for the self check profile.) I just chose a short name like sc01 to make it easy on myself.**
6. Select whether you want the self-check machine to send the following to Alma:
 Error correction – Select Yes for Alma to send/receive sequence numbers and checksums as part of the relevant messages. If this capability is enabled on the self-check machine, it must be enabled here as well. If you do not want to use this option, select No and turn it off also on the self-check machine.
 Alert messages
 Item transfer messages (not currently supported) **I clicked yes for the first 2 and no on the last one as it doesn’t sound familiar to me and is not anything we do at the self checkouts.**
7. From the SC language drop-down list, select the language in which Alma and the self-check machine communicate.
8. In the Retries allowed and Timeout period fields, enter the number of times you want Alma or the self-check machine to try to send a message following a failure of the first message to reach its destination, and the amount of time, in seconds, between each retry.
 Note that the recommended number of retries allowed is 2-5 and the recommended timeout period is 5-7. **I arbitrarily chose 2 and 5. No special reason why i chose these other than that if there are problems connecting to the self check, i want it to be quick so I can quickly figure out what’s wrong.**
9. Select the actions to be supported (Yes/No) between Alma and the self-check machine. (Note that Return message is not currently supported.)
 If you are using a 3M self-check machine, the checkin option must be set to Yes, due to a 3M requirement for enabling initial communication. If you do not want the check-in action to be allowed, ensure that you block it when configuring your 3M self-check machine. **It seems counterintuitive to click yes on this setting if your machine doesn’t allow checkins but it’s super important to click yes on this. I also clicked yes for checkout and renew but not for fee payments or returns as we don’t support that on our selfchecks at this time.**
10. From the Extension type drop-down list, select Extended fines and fees (Extended check-in is not currently supported) to enhance your self-check messages (SIP2) with additional fields. This option includes the following elements for each open charge in the SIP2 Patron Information Response message and allows self-check users to view this information (if available) when requested:
 EB - Barcode of the item that is linked to the charge (such as for an overdue/lost item)
 ET - Title of the item that is linked to the charge
 EC - Cash transaction type code
 ED - Cash transaction type description
 EF - Sum
 EK - Fee ID
 BZ - Payment transaction number
 Not all self-check machines support this option. This option should not be selected for self-check machines that handle only loans and returns (and not payment). **I didn’t put anything in this area as it seems more related to fines and fees payment and we currently do not support this in our machines.**
11. From the Item Identifier drop-down list, select the type of ID—Barcode, Call number, or Item ID—used to match physical items when incoming messages contain item IDs. **We use barcodes as our item identifiers.**
12. Under Authentication required, select Yes if you want the patron to be required to supply a password. (Note that the PIN code can be updated by the patron in Primo only if the use\_pincode\_for\_selfcheck\_machine parameter is set to true in the User Management Configuration > Configuration Menu > Other Settings Customer Parameters table.) **Also important to click yes on if you currently require people to sign in with a password on the selfcheck.**
13. For a secure TCP connection, click Download Certificate to download and save the certificate so that it can be used when configuring Stunnel (see step 3 in the introductory section above).
 Self-Check Integration Profile Definition – Page 2
 Click Save. The profile you configured appears in the Integration Profile List.**Once you click save, go back into the profile you just created and 3 tabs come up: general information, actions and contact information. Click default if this profile will be the default self check profile. The Actions Tab will show you the “download certificate” button. You will need this for setting up Alma to connect to the selfcheck via Stunnel. Make sure to download the certificate and save it to a secure spot on your machine. For the contact information tab, just add whoever will be the person who will be monitoring or administering the system.**

To associate a self-check profile with a circulation desk:

1. On the Fulfillment Configuration page (Fulfillment > Fulfillment Configuration > Configuration Menu), select the library whose circulation desk you want to associate with the self-check profile from the *You are configuring* drop-down list at the top of the page, and then click Circulation Desk under Library. The Circulation Desks List page opens. **Make sure that this desk doesn’t have a reading room associated with it. If it does, the selfcheck won’t be able to check out any items to patrons.**
2. Select Actions > Edit for the circulation desk you want to associate with the previously defined self-check profile, or click the Add Circulation Desk button to create a new circulation desk with which you want to associate the self-check profile.
3. On the Circulation Desk – General Information page, under Self-Check Information, select the *Has self-check check* box and select a previously defined self-check profile from the Integration profile drop-down list. The password for the self-check machine is automatically listed in the Terminal password field. (For information on the other fields on this page, see Configuring Circulation Desks.) Click Save to store your changes to the circulation desk. **I left the password as is because I wasn’t sure what it does or why it’s needed. General practice is to leave settings alone unless you 1. Know what the setting does. Or 2. Alma tells you what the setting does and you can make an educated decision from the information it provides you.**

From here, you are ready to set up your machine to communicate with Alma. If you have multiple machines, you will have to do this twice as far as I know. I didn’t try it any other way.

Important note: the selfchecks I was testing on hadn’t been updated in 3 years. Check to make sure your machine is up to date. It’s good to practice this in case there are any machine-related issues that might be fixed with an update. It also makes your machine more secure.

**Installing Stunnel on a Windows Workstation**

1.Go to the Stunnel downloads page to obtain the latest version of Stunnel: https://www.stunnel.org/downloads.html.

2.Download and run the latest stunnel-X.YY-installer.exe file.

3.When presented with the license agreement, click I Agree

4.Select the default installation options and click Next. **For this, just click the checkbox for everything.**5.Select the desired installation location and click Install. **Note: unless you have a place you typically put this stuff it will be in your program files area on your C: drive.**During the installation process, a command line box popped up asking to configure things like a country name. The answers to these questions are used to create the initial certificate file for Stunnel. Since you download the certificate from Alma, there is no need to provide real answers. Enter a period (.) for each question to leave it blank.

 **Configuring Stunnel to Run as a Windows Service**
To ensure that Stunnel is always running and starts when Windows starts, you may want to install Stunnel as a Windows service.

1.Open a command prompt and go to the directory in which Stunnel is installed. **You will need to know some basic windows commands.**

**cd\**

**cd program files (x86)**

**cd stunnel**

2.Execute the following command: stunnel.exe –install. **Just type** **stunnel.exe -install**

**Note: it was at this point I received some errors. It said “not a valid win32 application” when i tried to install. That day, I had been having some issues with the wired connection in our building. So i figured the file was probably corrupted in the initial download. I had to uninstall the service which just meant I had to go into the program file and click the uninstall.exe. I redownloaded Stunnel and reopened command line then repeated the last series of commands.**

**cd\**

**cd program files (x86)**

**cd stunnel**

**stunnel.exe -install**

**I received an error message saying ‘stunnel.exe’ not recognized as an internal or external command, operable program or batch file. I navigated to the program file to see why it wasn’t recognizing that the file was there. It had disappeared, which was strange because I knew I had successfully downloaded and installed it. I had a hunch that it was located somewhere else and found the stunnel.exe file in the bin folder. I don’t know why this is the case and I don’t care.**

**Once i figured this out, I typed cd bin which took me into that file area.**

**I typed stunnel.exe -install and the service installed successfully.**

3.Click OK.

4.From Control Panel - Administrative Tools, open the Services console.

5.Confirm that Stunnel is installed and configured as an Automatic startup type. To change the service settings, right-click the service name and click Properties

**Configuring Stunnel**

To configure Stunnel to communicate with Alma:

1. Double-click the Stunnel icon to start Stunnel.
2. Copy the certificate file to the directory in which Stunnel is installed. **I just navigated to the where the stunnel.exe file is located and copied the client.pem file to there.**
3. Select **Edit stunnel.conf** from the Configuration menu.
4. Delete the existing contents of the stunnel.conf file and paste the contents ExL has on the website. **Just need to point out here that you will need to make some minor adjustments to the stunnel.conf file, specifically in the integration profile. Edit based on your institution’s specific needs. You will want your own alma instance under connect and whatever port you will use. I just used the default 5001 port. Speak to your network administrator if you are unsure. Also for clarification, it’s asking for the full file pathway for the key/cert. So wherever your client.pem file is located, put the full file pathway or stunnel will not be able to locate the certificate. Also, for connect, only use the** [**https://na03.alma.exlibrisgroup.com**](https://xxxx.alma.exlibrisgroup.com) **address for the connect portion. Don’t include anything like your specific institution’s alma code. It just needs to be able to connect to Alma as a whole.**
5. Click Save and close the file.
	1. In certain situations, you must create multiple connection definitions in the stunnel.conf file. If you receive multiple client certificates from your Alma implementation engineer, add each one with a different name to the Stunnel installation directory, Then copy the entire [Integration Profile 1] section and edit the appropriate values, including the certificate file name and accept port*.* For example, you can add a second [Integration Profile 2] using client2.pem certification and accept port of 5002 **Don’t worry too much about this unless you’ve been specifically instructed to do this. I have 2 machines I am doing this from and there is no need to add a second integration profile for most instances.**

**Testing that Stunnel is Running Correctly**

 Confirm that the console displays a confirmation that it is running correctly. You should see a line in the stunnel log saying that the configuration was successful. To further test that stunnel is running correctly, open up command line again and type telnet xx.xxx.xx.xx 6443(your stunnel ip and the port number with no colon)

If Stunnel is not operating correctly, an error message, such as the following, is displayed:
 C:\ >telnet 10.1.116.102 5001

 If Stunnel is operating correctly, the command prompt clears and you connect to Stunnel. **Note: It will look like a blank page.**

**Configuring the Self-Service Machine to Communicate with Stunnel**

1. Configure the self-service machine to send traffic to the IP address of the workstation on which Stunnel is running and configure the port to the value configured in the Stunnel configuration file.

For 3M self-service machines, update the following two parameters under the self-service machine administration:
Integrated Library System (ILS) Host IP Address – Enter the IP address of the workstation that is running Stunnel.
ILS TCP Port Number – Enter the port that you specified during Stunnel configuration (such as 5001).
The self-service machines are configured to communicate with the Stunnel workstation and not directly with the library management system (the ILS).

**It was at this point that I had a great series of issues spanning over 2 days of trying to figure out what was wrong. First, I found out that the technicians at SJSU had not set up the static IP address like I originally thought they did. I fixed this by having each selfcheck set up with a static IP, NOT a dynamic IP.**

**Second problem: issues with the port number. The log would give me a “signal pipe is empty” message. For whatever reason, 5001 and 5002 were not working for me so I switched to 5004 and this seemed to fix the problem.**

**Log error:**

 **2016.09.07 15:56:09 LOG3[main]: bind: Address already in use (WSAEADDRINUSE) (10048)**

**2016.09.07 15:56:09 LOG3[main]: Error binding service [Integration Profile 1] to 0.0.0.0:5001**

**2016.09.07 15:56:09 LOG7[main]: Signal pipe is empty**

**Third issue: Selfcheck still not connecting. It kept giving me error messages with my stunnel.conf file. Said something along the lines of:**

**2016.09.07 16:27:50 LOG6[0]: Certificate verification disabled**

**2016.09.07 16:27:50 LOG6[0]: Certificate verification disabled**

**Looked it up in the Alma-L listserv and found out that your client.pem file has to be in the \conf directory rather than in the \stunnel directory. This seems to be a super important piece of information that is not listed in the documentation. BEWARE OF THIS. I also moved the stunnel.conf file to the \conf directory just in case that might cause issues too.**

**Fourth issue: still not connecting BUT got a different error. This time the error message the selfcheck gives me when it turns on is different. It says “circulation system operation failure - Business layer logic error - report to software service - ERR\_SIPBL\_ILS\_CAPABILITY” Again, i tried the Alma-L listserv to see if someone had reported this same issue. It turns out they had. I found out there is a tiny little checkbox in the selfcheck administrative area that needed to be unchecked. Under Network > Sip Communications > uncheck Error Detection > save settings > restart the selfcheck.**

**Bonus issue: Problem with Ithaca280 printer. In this instance, I highly suggest calling Bibliotheca support. I was able to get it working, but it involved some scary driver reinstalls that left me sweating and thinking I had broken the system. Don’t be dumb like me, just call support.**

**Current issues**

Currently the system is set up to accept a pin number like the selfcheck did. Right now it can’t be set automatically, it will have to be set manually from either Primo by the patron or by a staff member in Alma. I am currently looking into seeing if this is something we can connect to via shibboleth but no further news on that front.

**Appendix A: On remote log ins**

If you’re lazy like me and don’t want to leave your desk to go back and forth between logging into the selfcheck and testing there and going back to your desktop to do other work while you wait for testing to complete, there is a way to do this without installing any software such as pcanywhere, which is a paid program that 3M techs use to do remote assistance but is not necessary for our purposes.

1. First, make sure you have the IP address for your machine. You can find it by clicking start > run > type cmd > hit enter > then type ipconfig and hit enter. Look for the IPv4 Address and write down the 10 digit number you find there. It should look something like xx.xxx.xxx.xx
2. Now you will want to find out what your administrator password is. Go to Start > search regedit > Click HKEY\_LOCAL\_MACHINE > Click SOFTWARE > Microsoft > windows NT > CurrentVersion > WinLogon > DefaultPassword > record what the default password is. If it’s not set, make sure to set one. http://www.isunshare.com/windows-7-password/windows-7-admin-password-reset.html
3. Once you find your default password, you will need to disable your auto log in function if you currently have your selfcheck set up to log in automatically when it is turned on. The reason for this is that windows does not allow concurrent log ins for the same user from remote desktop connections. I believe it’s some sort of licensing issue and is hardcoded into the system. There are illegal patches available to get around it but **don’t do this**. It’s easy to turn off and on without doing anything illegal. Go to start > search for **netplwiz.** Uncheck the box that says “Users must enter a user name and password to use this computer.” Click Apply, then click okay. It will ask you to type in your default password.
4. It should automatically log you out. If it doesn’t, just go to start and click log off. Type the default password you recorded in step 2.
5. You have now turned off auto log in so the system won’t automatically log you out when you connect remotely. Make sure to do this with a machine you aren’t currently allowing patrons to use. You can also restart your selfcheck machine to make sure the log in screen comes up.
6. Now you are ready to connect remotely. On your desktop, go to start and search for “remote desktop connection”. Type in the computer’s IP address. It will likely ask you for administrator user name and the default password. If you don’t have one set, make sure you do because RDC doesn’t allow remote desktop connections with a blank password. A certificate validation area will likely pop up next. Click Yes. You should see your computer’s remote screen after you do this and now you can easily do configurations from the comfort of your own desk.

To enable auto log in after you are done configuring and testing, go to Start > search > and type

**netplwiz**

1. Check the “Users must enter a user name and password to use this computer” box.
2. Click on the user account name, that you want to have automatically log on at startup, to highlight it. (Should be the administrator password not the 3mtech account)
3. Click apply and then click ok
4. Enter the default password for the user account
5. Restart your machine to ensure it logs in and starts up automatically. Note: it’s possible to do this from the registry editor as well but i found this to be slightly more easy to follow with a lot fewer potential problems.

**Appendix B: On connecting multiple selfchecks**

A while back I saw a discussion unfold on the listserv about connecting multiple selfchecks onto one instance of Stunnel. I chose not to do this because I don’t have direct server access and I don’t want all of the selfchecks to go down if one of them goes down. Here are some comments from the discussion on the Alma-L listserv:

*From Simon:*

“Most of the information for setting up self checks is available at http://knowledge.exlibrisgroup.com/Alma/Product\_Documentation/Alma\_Online\_Help\_(English)/Integrations\_with\_External\_Systems/040Fulfillment/060Self-Check\_Machines. The main thing to decide when setting up multiple machines is whether to run Stunnel on each self check or on a server that each of the self checks connect to. The advantage of the server approach is that you only need to maintain one instance of Stunnel but the disadvantage is that if it goes down all your self checks will become unavailable + the communication between the self checks and Stunnel is insecure.”

*From Ian:*

“We migrated to Alma this summer and have 6 3M V series across 2 libraries. We were advised by Ex Libris to have a second Alma circ desk at each library to handle the self-service transactions for ease of management. We have 1 stunnel server which all the V series communicate with (or will do).

 No real gotchas to warn you of – but be aware of network security. Our IT Service people are obsessed with this and so the V series have their own VLAN. Getting this bridged across to our second smaller library has proved very difficult, hence our main library V series have been live for nearly a month and the V series at the health library still isn’t working (and semester is getting worryingly close!). Be prepared for short periods of downtime once a month for the monthly updates – these are usually in the early hours of a Sunday morning for us, so although we’re open 24/7 during semester it shouldn’t be a major problem.

 Good things? We moved over from Millennium, which couldn’t manage email receipts from the V series, but Alma does this out of the box. I was also quite pleased by the way it handled our cash-based fine payments almost of the box as well.

 The worrying thing is the future of 3M self-service hardware after the takeover by Bibliotheca, but this may be different in your part of the world.”

I responded to Ian:

“

Thank you for the response. There was a discussion a while back about this that I had saved but I couldn't seem to find it. We're currently in the process of switching to Alma and it was something I wasn't sure about. Ian- are you saying to have a second circ desk associated with the library that has the selfcheck? The ExL documentation I am using just said to click the checkbox that says "circ desk has selfcheck" and associate it with the default circ desk. Do you happen to know why Ex Libris suggested you set it up that way?”

Who explained further:

“ Yes, we have 2 circ desks for each of our libraries, for the counter and the selfchecks. Our Ex Libris consultant recommended doing it that way for 2 reasons: primarily that it enables you to separate your statistics for them, but also that it gives the potential for having slightly different configurations for each. Being able to distinguish the proportion of self-service use of the library has always been of importance to us: last year we were around 90% self-service. Our 3M V series selfchecks do give quite good stats individually, but doing it this way avoids having to sum them together regularly. Ask me in a year and I’ll tell you whether it has been worthwhile!”

So basically, from my understanding, it’s not necessary to do this if you’re not super interested in getting detailed stats about your selfcheck from Alma as the V-series seems to give good stats on its own. Follow this advice at your own risk.

**Appendix C: Current contents of the SJSU stunnel.conf file**

; \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

; \* Global options \*

; \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* ;

; Debugging stuff (may useful for troubleshooting)

debug = 7

output = stunnel.log ;

;Disable FIPS mode to allow non-approved protocols and algorithms

fips = no

;\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

; \* Service defaults may also be specified in individual service sections \*

; \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

; Disable support for insecure SSLv2 protocol

options = NO\_SSLv2

 [Integration Profile 1]

key = C:\Program Files (x86)\stunnel\config\client.pem

cert = C:\Program Files (x86)\stunnel\config\client.pem

client = yes

accept = 5004

connect = na03.alma.exlibrisgroup.com:6443

TIMEOUTclose = 0

TIMEOUTconnect = 200

TIMEOUTidle = 86400