IBM Security Guardium

Guardium UI Login using a Smart card

Overview

Guardium Smart card support meets the United States government mandate that all vendors must support multi-factor authentication for user access. Smart card authentication is supported only for access to the web-based Guardium user interface (UI).

Details of the multi-factor authentication requirement are found in the Identification and Authentication (Organizational Users) (IA-2) section the Security and Privacy Controls for Federal Information Systems and Organizations (NIST Special Publication 800-53) document. NIST 800-53 is available through the NIST web site: https://www.nist.gov .

Government applications refer to Personal Identification and Verification Cards (PIV). Civilian applications refer to Common Access Cards (CAC). PIV and CAC cards have different certificate authorities, but the cards are otherwise the same.

Guardium Smart card support meets the HIGH confidence PIV assurance level described in the PIV Cardholder Authentication (6) section of the Personal Identity Verification (PIV) of Federal Employees and Contractors (FIPS Publication 201-2) document. FIPS 201-2 is available through this NIST web site: https://www.nist.gov .

Prerequisites

The device requires the following:

- Access to the Guardium UI via a web browser that can access the Smart card certificate
- A Smart card reader
- A valid PIV/CAC card

Configure the association of users with Smart cards

Learn how to correctly associate Guardium users with Smart cards.

About this task

This task describes how to correctly associate the information on a Smart card with a Guardium user.

Before you begin

Create Guardium users to associate with Smart cards. If you want to associate existing users with Smart cards, you do not need to create any new users. For more information about user creation and access management, see Access Management Overview.

1. Login to the Guardium UI as the admin user.
2. Navigate to Setup > Tools and Views > Portal
3. Under the Authentication Configuration section, select the Smart Card option. If the Smart Card option is not present, verify that the Smart card patch is installed.
4. In the Regex Match Pattern field, provide a regular expression (regex) that matches user information on a Smart card.

Configure the Mapping of user to Smart card

Create users

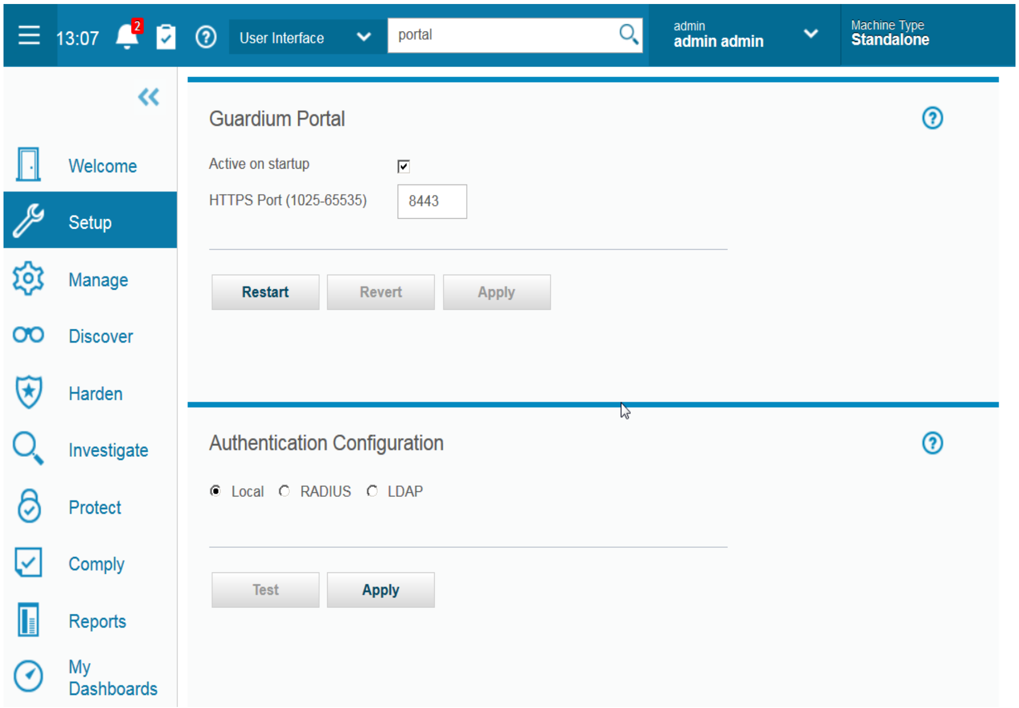
The Guardium application provide various ways for users to be created. It doesn't matter how your users are created, and once you configure your web to use the Smart card for authentication it only uses the Smart card credential to establish SSL/TLS communication (Guardium site uses https).

Here is an example how manually create a user:

1. Login as Accessmgr on CM
2. Select Access -> User Browser
3. click Add user button
4. Add Username Test Cardholder X
5. Add password twice
6. Enter first name and lastname same as user
7. Click Add User button

Now you will configure the mapping so when a Smart card is present the information on the Smart card will be correctly mapped to a user in the system.

1. Login as Admin from CM or standalone.
2. After you login, go to Setup > Tools and Views > Portal



Guardium Portal

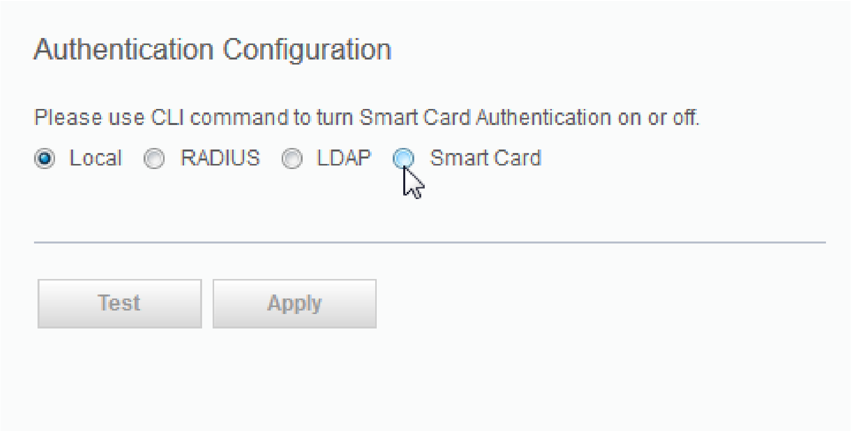
Active on startup ☑

HTTPS Port (1025-65535) 8443

Authentication Configuration

● Local ○ RADIUS ○ LDAP

If you see the following it confirms that you indeed have the Smart card support patch installed.



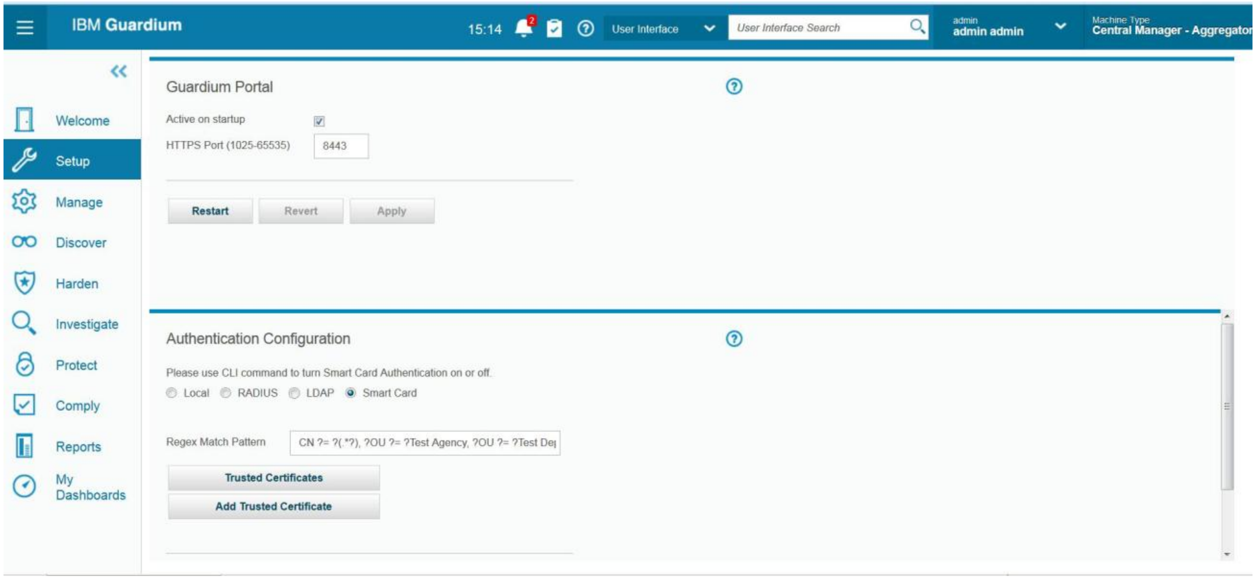
Authentication Configuration

Please use CLI command to turn Smart Card Authentication on or off.

● Local ○ RADIUS ○ LDAP ○ Smart Card

Now use a regular expression to match the user information on the Smart card.

Here is an example - see Regex Match Pattern.



Guardium Portal

Active on startup ☑

HTTPS Port (1025-65535) 8443

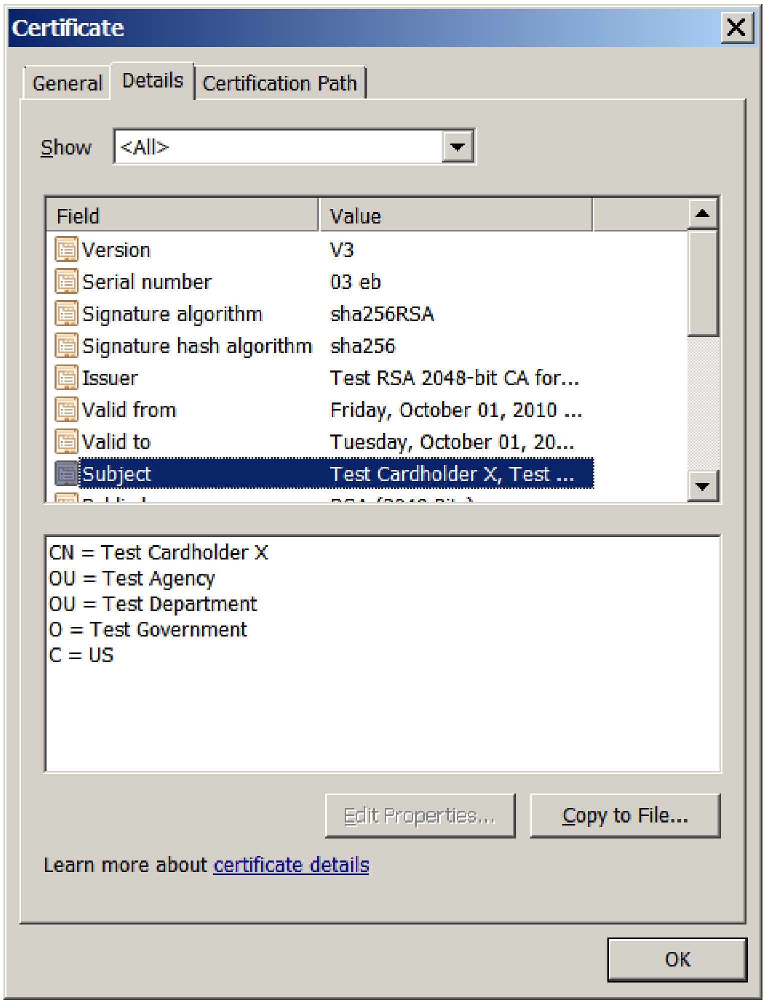
Authentication Configuration

Please use CLI command to turn Smart Card Authentication on or off.

○ Local ○ RADIUS ○ LDAP ● Smart Card

Regex Match Pattern CN ?= ?(.*?), ?OU ?= ?Test Agency, ?OU ?= ?Test Dep

This works with a Smart card with client certificate. The client certificate you selected to send to the webserver to establish HTTPS. On the Smart card you selected this client certificate to give to the webserver when the server requests it, which is exact what happens when this feature is enabled. The client certificate has the follow details which you can see in the certificate details from the browser.



Field	Value
Version	V3
Serial number	03 eb
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	Test RSA 2048-bit CA for...
Valid from	Friday, October 01, 2010 ...
Valid to	Tuesday, October 01, 20...
Subject	Test Cardholder X, Test ...

CN = Test Cardholder X
OU = Test Agency
OU = Test Department
O = Test Government
C = US

In this example you can use one of the following patterns. They both will match the mapping. Pattern 1 is more exact. Pattern 2 depends on your purpose, you can write your own to match your needs. You need to work with someone who is familiar with the data on the Smart card to write efficient mapping patterns.

Pattern 1:

CN ?= ?(.*?), ?OU ?= ?Test Agency, ?OU ?= ?Test Department, ?O ?= ?Test Government, ?C ?= ?US

Pattern 2:

CN ?= ?(.*?)

Both of the examples will get the value for CN attribute in the certificate subject which you can see by examine the detail of the certificate from the browser. In this case it is Test Cardholder X. Configure this pattern correctly is probably the most important part to make sure the authentication on Smart card is successful.

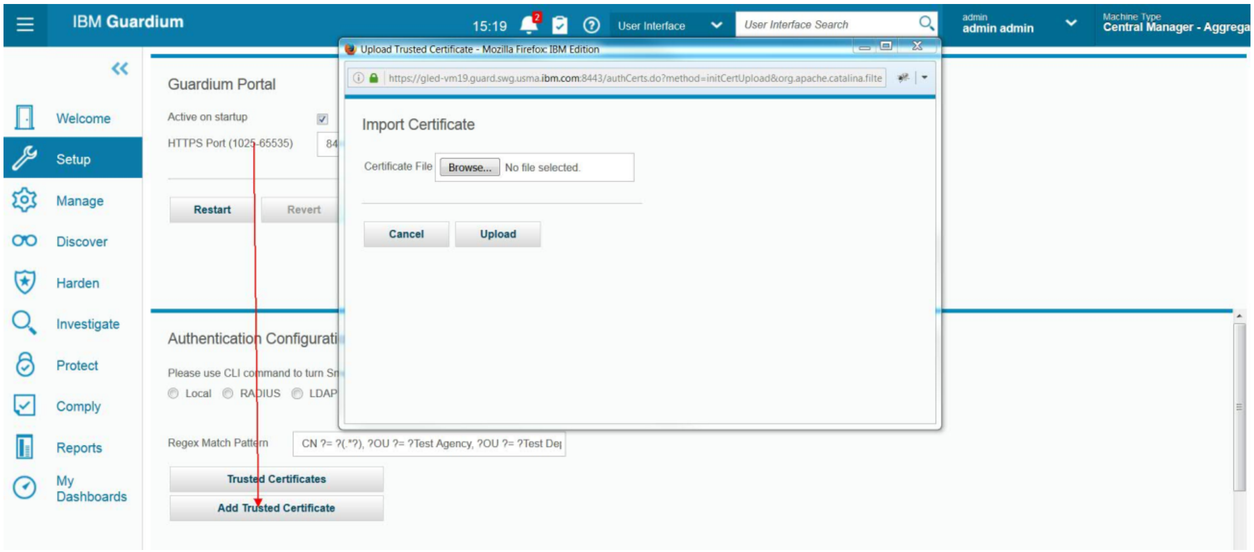
Note that the regex validation tool currently available for other modules is not available for this purpose. (see Troubleshooting section, items 2 and 3).

Now save it. Note, you are not done yet and you need to enable it from CLI since part of the enablement can only be done after the server is shut down, during which there is no GUI.

Before you leave GUI for the CLI part, you need to upload the root CA certificate to the trust store. (See section Upload the root CA's certificate to web server's trust store.)

Upload the root CA's certificate to web server's trust store

This part describes how you upload the root CA's certificate into the trust store used by the GUI. You can obtain the root certificate from one of the following sources.



Guardium Portal

Active on startup ☑

HTTPS Port (1025-65535) 84

Authentication Configurati

Please use CLI command to turn Sr

○ Local ○ RADIUS ○ LDAP

Regex Match Pattern CN ?= ?(.*?), ?OU ?= ?Test Agency, ?OU ?= ?Test De|

https://gled-vm19.guard.swg.usma.ibm.com:8443/authCerts.do?method=initCertUpload&org.apache.catalina.filte

Import Certificate

Certificate File No file selected.

If you do not have the root certificate of the CA that signed the certificates on the Smart cards, you can export a root certificate from a CA-signed user certificate or a Smart card that contains one.

We assume you obtained the certification either by having it given to you by the customer or exporting it from a Smart card using certification management tools such as certMgr.exe or tools like open SSL.

The public root certificate of a trusted CA. This is the most common source of a root certificate in environments that already have a Smart card infrastructure and a standardized approach to Smart card distribution and authentication.

Select a certificate to use for Smart card authentication. The signing chain lists a series of signing authorities. The best certificate to select is usually the intermediate authority above the user certificate.

Enabling the feature from CLI (can only be done in CLI)

To check the status, use the CLI command, show system websmartcard.

Here you'll see it's not enable and it tells you how to turn it on:

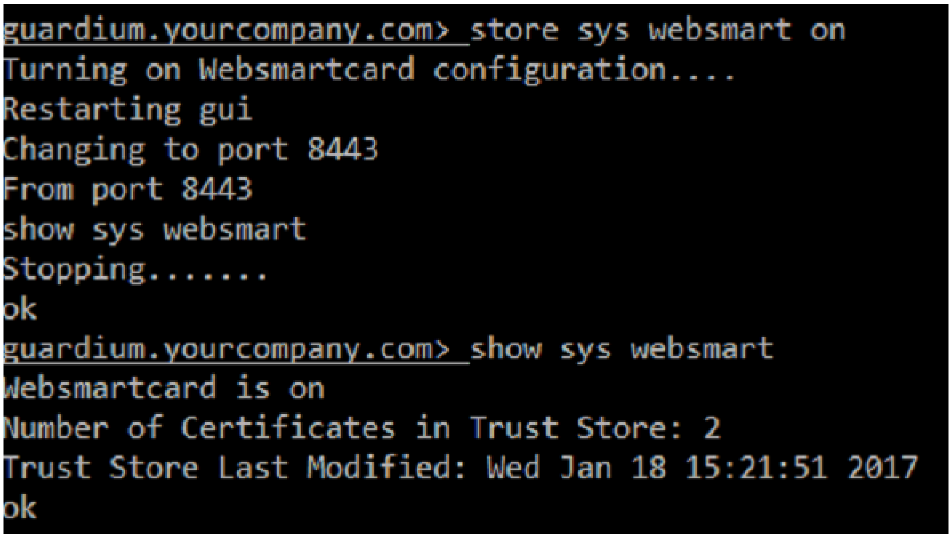
```
CLI> show system websmartcard

Portal configured for Websmartcard, run 'store system
websmartcard on'

Number of Certificates in Trust Store: 1

Trust Store Last Modified: Wed Jan 18 15:21:51 2017
```

Now let's enable the feature and do a check afterwards:



```
guardium.yourcompany.com> store sys websmart on
Turning on Websmartcard configuration....
Restarting gui
Changing to port 8443
From port 8443
show sys websmart
Stopping.......
ok
guardium.yourcompany.com> show sys websmart
Websmartcard is on
Number of Certificates in Trust Store: 2
Trust Store Last Modified: Wed Jan 18 15:21:51 2017
ok
```

In case you need to turn it off for, use:

```
CLI>Store system websmartcard off
```

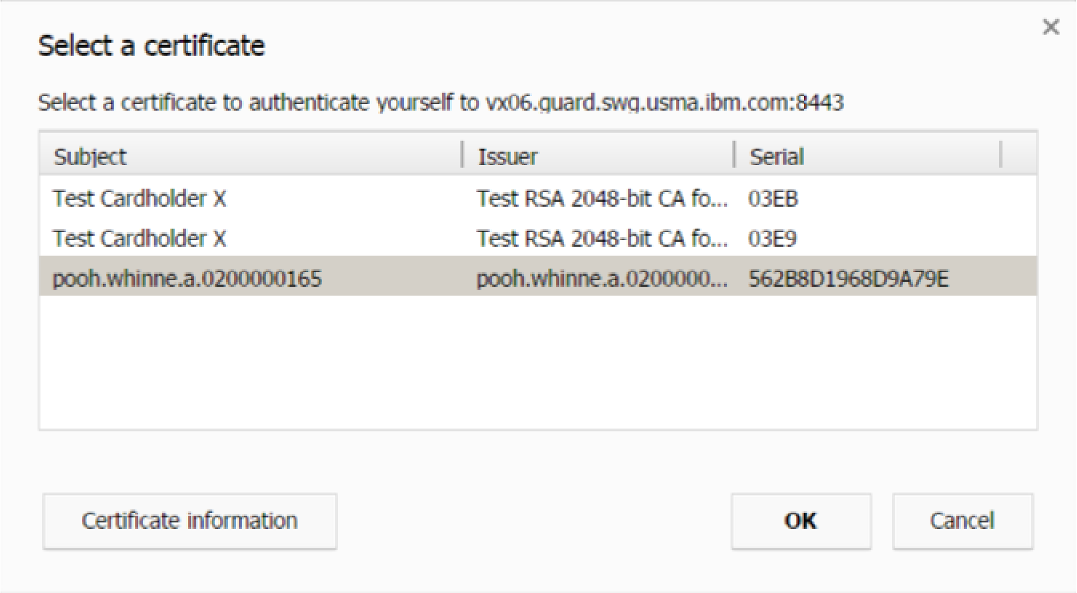
With this command the feature is turned off and GUI is automatically restarted with the system using local authentication. This is also useful when you first deploy the system and the regular expression you set is not quite write and you see error.

Note, while the Smart card authentication is used to authenticate, the access control (for example, what module a user has access, what navigation the user has is still done through the same way as without Smart card authentication.

After enabling the feature:

Once the feature is enabled you can only access the site with a valid Smart card (PIV, CAC etc.)

Now when you visit the GUI site, you’ll see the following prompt:

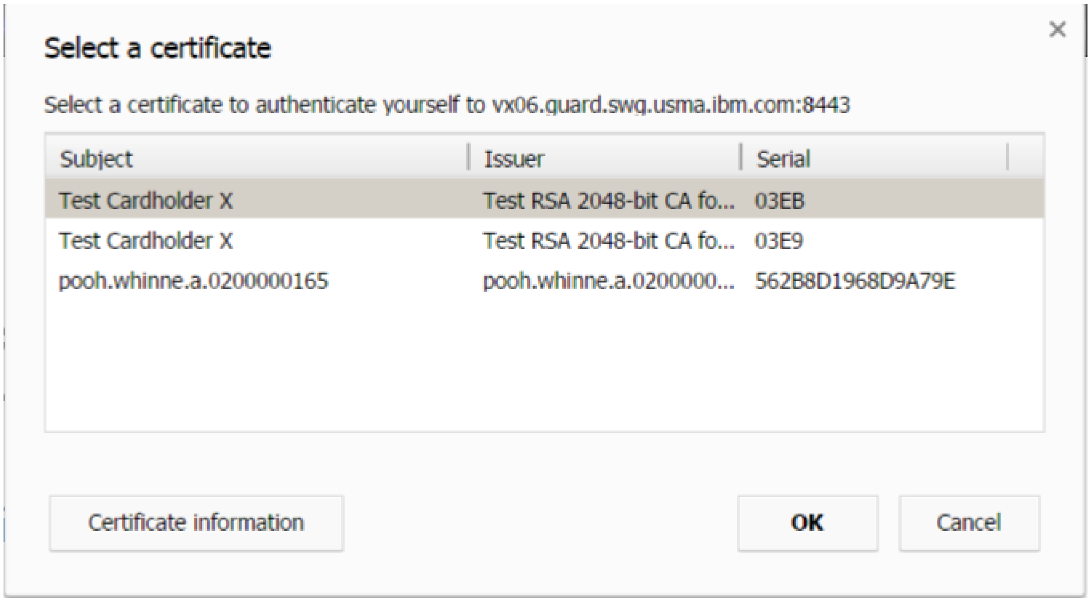


Select a certificate

Select a certificate to authenticate yourself to vx06.guard.swg.usma.ibm.com:8443

Subject	Issuer	Serial
Test Cardholder X	Test RSA 2048-bit CA fo...	03EB
Test Cardholder X	Test RSA 2048-bit CA fo...	03E9
pooh.whinne.a.0200000165	pooh.whinne.a.0200000...	562B8D1968D9A79E

Another example:



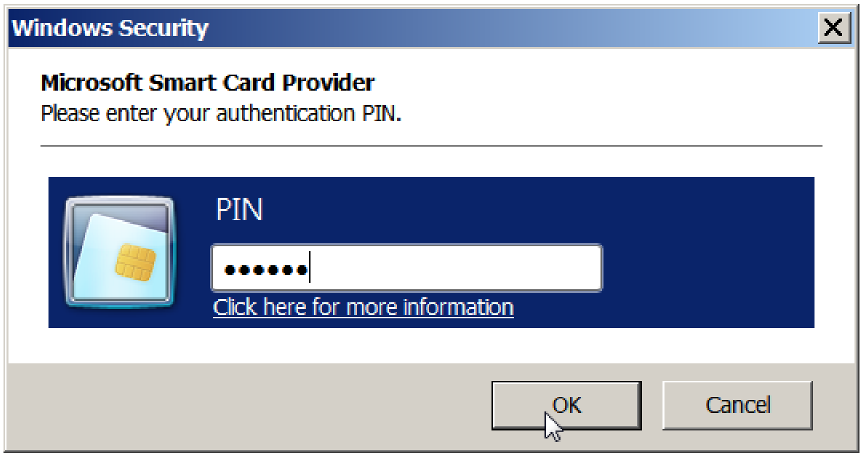
Select a certificate

Select a certificate to authenticate yourself to vx06.guard.swg.usma.ibm.com:8443

Subject	Issuer	Serial
Test Cardholder X	Test RSA 2048-bit CA fo...	03EB
Test Cardholder X	Test RSA 2048-bit CA fo...	03E9
pooh.whinne.a.0200000165	pooh.whinne.a.0200000...	562B8D1968D9A79E

The above details are for an admin to set it up. As for end user, if it is set right, the user just needs to put the card in and the user will go straight to the site content.

For a user with a valid Smart card, when the user load the websites, the browser will prompt for Smart card pin. This pin allows the client certificate on the card is access when requested.



Windows Security

Microsoft Smart Card Provider

Please enter your authentication PIN.

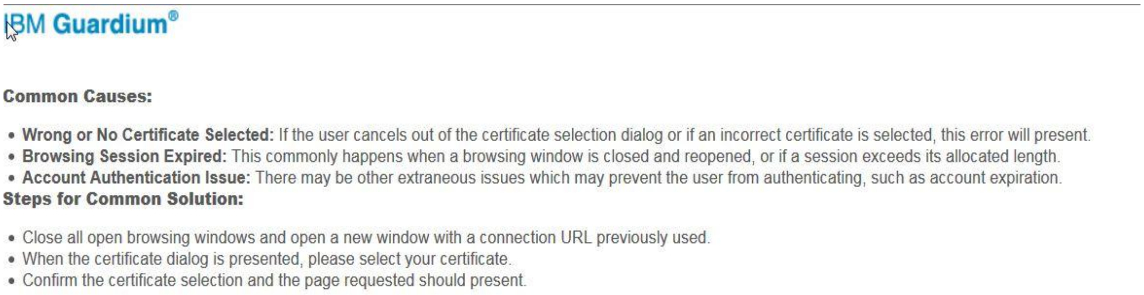
PIN: ●●●●●●

After the pin is provided, the regular Guardium login page will display with the user field pre-filled with the login extracted from the Smart card. Note there is no password used here. The only thing you see in the user field is the extracted user place holder for mapping.

For example, if the certificate are valid and the root CA of the Smart card issuer for Test Cardholder X is loaded in Guardium web server (See section Upload the root CA's certificate for how to do it), the user field will be prefilled with Test Cardholder X and prompt you for the Smart card pin. This is to access the client certificate on the Smart card. The client certificate stays on the Smart card and you cannot export it into a file. You may see the prompt twice and just provide the pin.

Troubleshooting or recovery scenarios

1. After the feature is enabled, when you load Guardium URL, you see an error page shown as follows:



Common Causes:

- **Wrong or No Certificate Selected:** If the user cancels out of the certificate selection dialog or if an incorrect certificate is selected, this error will present.
- **Browsing Session Expired:** This commonly happens when a browsing window is closed and reopened, or if a session exceeds its allocated length.
- **Account Authentication Issue:** There may be other extraneous issues which may prevent the user from authenticating, such as account expiration.

Steps for Common Solution:

- Close all open browsing windows and open a new window with a connection URL previously used.
- When the certificate dialog is presented, please select your certificate.
- Confirm the certificate selection and the page requested should present.

Diagnostic: Most likely, your configuration of the matching regular expression is not right or you don’t have a valid certificate on the card.

2. You created a matching Regex and it doesn't seem to be working. You remember that Guardium has a regex validation tool and used it thinking that if it works in the tool, it's a good Regex. Unfortunately, while the test is successful in that tool, the Regex pattern doesn't work for Smart Card Configuration.

Diagnostic: That tool is to find if an expression can be found inside a text paragraph. So it won't work in this case. This configuration is to extract a piece of text from the certificate text as displayed in the subject as shown in certificate details.

3. You didn’t get prompt from the browser to select a certificate at all.

Diagnostic: PC/laptop is able to install the card reader and the Smart card. A copy of the certificate in the Smart card gets copied to the certmgr in Windows OS. However, when accessing the site, browser (IE or Firefox or Chrome) does not read the certificate. In other words, all the three browsers are unable to read the certificate and there is no prompt to choose the certificate.

This has been noted on all browsers on some laptops we tested. If this is the case, it’s not only happening to Guardium site. Other sites that requires Smart card to operate will also experience this. This is rare.

Solution: Contact the department that manages your Smart card.

= = = = = = == = == =