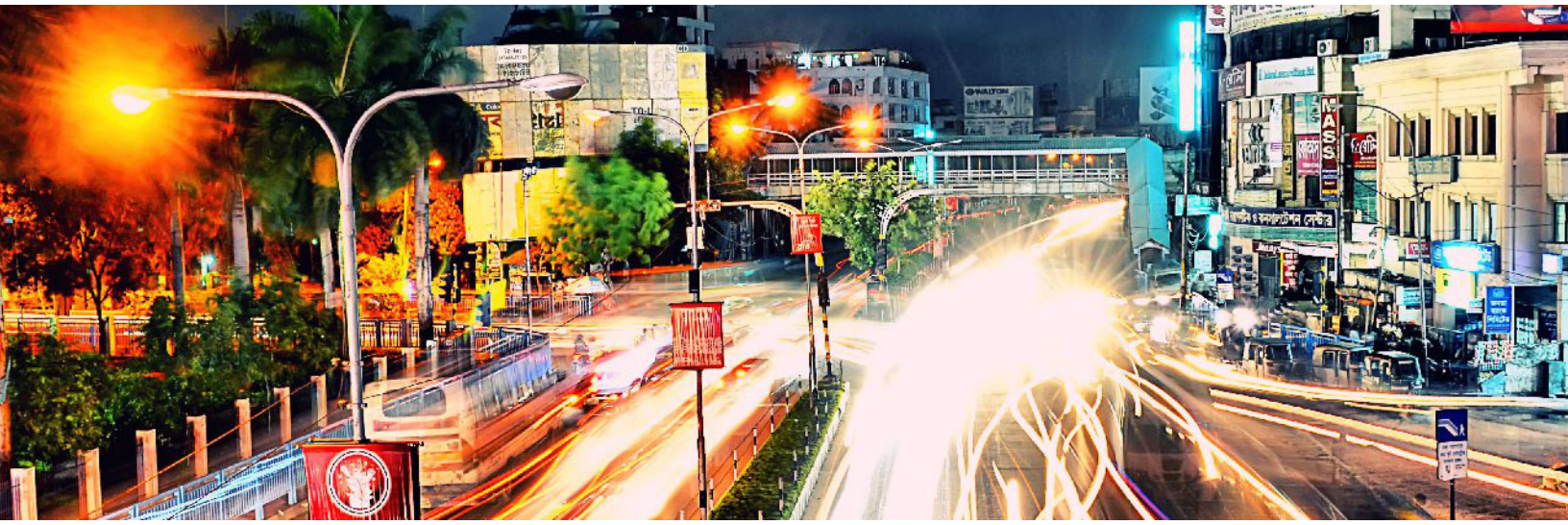
Creating and Using Security Keys



CyberSource®
A Visa Solution

CyberSource Contact Information

For general information about our company, products, and services, go to http://www.cybersource.com.

For sales questions about any CyberSource Service, email sales@cybersource.com or call 650-432-7350 or 888-330-2300 (toll free in the United States).

For support information about any CyberSource Service, visit the Support Center: http://www.cybersource.com/support

Copyright

Restricted Rights Legends

Trademarks

Revision: July 2020

Contents

Recent Revisions to This Document

Release	Changes
July 2020	Added Business Center URLs for India. Added SOAP section. Updated procedures to account for EBC2 changes. Fixed broken links.
October 2018	Updated the procedure for generating a Simple Order API security key. See Generating Simple Order Security Keys.
September 2016	Updated the Java browser plug-in version requirement. See Generating Simple Order Security Keys and Generating SCMP Security Keys.
May 2016	Added the duration of the Simple Order security key. See Generating Simple Order Security Keys.
August 2014	This revision contains only editorial changes and no technical updates.
March 2014	Updated the SCMP chapter to include instructions for Using eCert.

Simple Order Security Keys

The CyberSource Simple Order API uses public key cryptography to securely exchange information over the Internet. Before you can send requests for CyberSource services using the Simple Order API, you must create a security key for your CyberSource merchant account on the Business Center.

Generating Simple Order Security Keys

Context

The Business Center uses a Java applet to generate security keys.

The Java applet requires version 1.6 or later of the Java browser plug-in. If the applet fails to load properly, install the latest version of your browser and try again.

IMPORTANT: You must use separate keys for the test and production environments.

NOTE: A security key created in the Business Center for the Simple Order API is valid for two years.

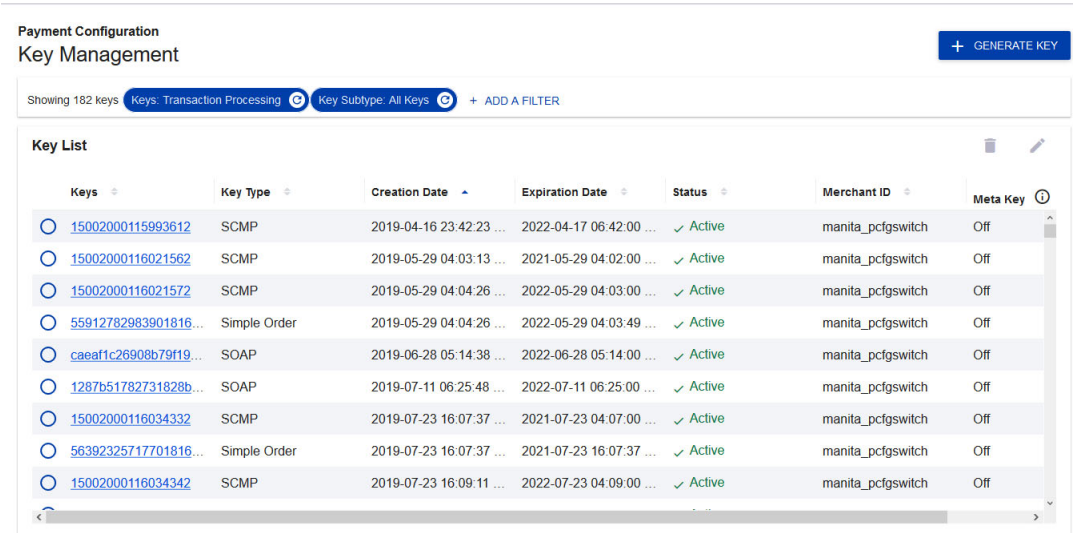
---

1 Log in to the Business Center.

- Test Environment: https://ebc2test.cybersource.com/ebc2/
- Production Environment: https://ebc2.cybersource.com/ebc2/
- Production Environment in India: https://ebc2.in.cybersource.com/ebc2/

2 Choose **Payment Configuration**  **> Key Management**.

3 On the Key Management page, In the upper-right, click the **+GENERATE KEY** button.



4 Choose **Transaction Processing**. Click **Next Step**.

5 Choose **Simple Order**. Click **Submit**.

6 When prompted to open a *simple_order.jnlp* file, choose **OK**. If a security warning appears, click **Continue**.

7 Click **Download**.

8 Click **Keep** in response to the security warning.

9 Open the file. A warning message might appear.

10 Click **Continue**. The application downloads.

11 Click **Run**.

12 Click **Generate Certificate Request**, and then **Continue**.

13 Within the **Save** dialog box, choose a location on the current server to save the key file. Be sure to use separate locations for the test and production environments. Be careful not to overwrite a key in the wrong directory. If you do not protect your security keys, the security of your CyberSource account might be compromised.

Importing Key File

Context

You must import a security key before you can view its serial number.

1. Find and double-click the key file name. The Certificate Import Wizard opens. Click **Next**.
2. The Wizard shows the path to the key file. Click **Next**.
3. Enter the password for the key file. The password is the merchant ID that you used to log in to the Business Center to generate the key.
4. Clear all check boxes. Click **Next**.
5. Ensure that **Automatically select the certificate store based on the type of certificate** is checked. Click **Next**.
6. Click **Finish**. A warning appears.
7. In the warning message dialog box, click **Yes**. A success message appears.

Verifying Serial Numbers

In the Business Center, you can view a list of the keys that you have generated. However, the keys are listed by their serial number, not their file name. If you are unsure which is the active key, you can view the serial numbers for your locally stored key files. Then you can match the locally stored keys to the information shown in the Business Center.

Viewing the Serial Number

Context

These instructions are written for Internet Explorer 11. Modify them as needed for your browser.

1. Open Internet Explorer.
2. In the upper right corner of the browser, choose **Tools > Internet Options**.
3. In the Internet Options window, click the **Content** tab.
4. In the Certificates area of the window, click **Certificates**. The Certificates window shows a list of the certificates that were imported.
5. Double-click on the key file that you imported in the previous section. The Certificate window for that file opens.

6 Click the **Details** tab. The window shows a list of fields and values, but the **Serial Number** field does not contain the correct serial number information. Instead, the **Subject** field contains the correct information.

7 Click the **Subject** field. The lower window displays the serial number for the key file.

SCMP Transaction Keys

The CyberSource SCMP API uses public key cryptography to securely exchange information over the Internet. Before you can send transactions to CyberSource by using the SCMP API, you must log in to the Business Center to create and download the following transaction key files for your merchant account:

File Name	Description
merchant_id.crt	Your public certificate file
merchant_id.pvt	Your private key file
CyberSource_SJC_US.crt	CyberSource server certificate file

NOTE: The Business Center uses a Java applet to generate security keys. The Java applet requires version 1.6 or later of the Java browser plug-in. If the applet fails to load properly, CyberSource recommends that you download and install the latest version of your browser and try again.

IMPORTANT: You must use separate key files for the test and production environments.

Generating SCMP Security Keys

Context

The SCMP API uses S/MIME standard cryptographic message exchange to guarantee privacy and provide strong authentication. SCMP security keys use a filename format of *merchant_id.crt*.

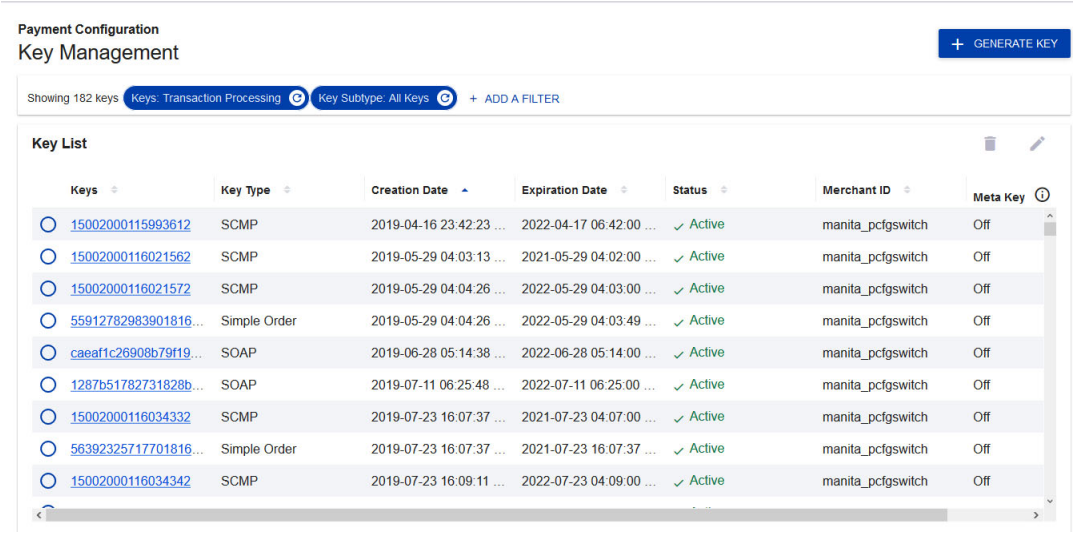
The JNLP component used when creating a key file requires Java Runtime Environment (JRE) to be installed on the system. If the JNLP component fails to run, visit the Oracle website to download the latest version of JRE.

1 Log in to the appropriate Business Center environment.

- Test Environment: https://ebc2test.cybersource.com/ebc2/
- Production Environment: https://ebc2.cybersource.com/ebc2/

2 Choose **Payment Configuration**  **> Key Management**.

3 On the Key Management page, in the upper-right, click the **+GENERATE KEY** button.



4 In the Select a key type dialog, choose **Transaction Processing**. Click **NEXT STEP**.

5 In the Select a key subtype dialog, choose **SCMP**. Click **SUBMIT**. The JNLP download begins.

6 When prompted, save the *scmp.jnlp* file.

7 Open the *scmp.jnlp* file and click **Run**. If the application does not run, you should update the Java Runtime Engine (JRE) on your computer. Restart the computer after updating the Java software.

Specifying Transaction Key Locations

After you download your SCMP API transaction key file, you must specify the key directory location so that your client application can find the directory when you send transactions to the CyberSource server. The following table describes how to specify the key directory location for each type of SCMP API client application. For more information, see the SCMP API Documentation and Downloads page.

SCMP API Client Type	Method to Specify Transaction Key Location
C/C++	The client searches for the keys in *ICSPATH\keys* directory path where `ICSPATH` is an environment variable that you must set. This applies to both Windows and UNIX. For additional options, see the documentation for your client.
.NET 2002, 2003	

SCMP API Client Type	Method to Specify Transaction Key Location
Java	Set the **ics.keysPath** property in the *ICSClient.props* file.

Using eCert

Context

CyberSource has a legacy application for generating security keys called eCert. The following eCert instructions are for Windows 7.

For security purposes, you must update your eCert certificate and private key at least every 12 months. CyberSource sends advance notice 60 days before your keys expire, followed by additional reminders until your keys are updated. You should regularly review your certificates and private keys to prevent any disruptions in transaction processing.

Security keys created for the SCMP API with the legacy eCert application are valid for one year. Keys created in the Business Center are valid for two years.

1. Navigate to the eCert Application page.
2. From the list of four application options, click Update to ECert Application windows v.5.0.1 to download the Windows version of the eCert application.

   If your website is hosted on a Linux server but you are generating the keys on a PC with Windows, use the Windows version of eCert.
3. When the File Download dialog box appears, select a location in which to save the file. Note the location and click **Save** to download the application.
4. When the download is complete, unzip and extract the *ecert-windows-5.0.1.zip* file.
5. Open the ecert-windows-5.0.1 folder that you just extracted. *Do not double-click on ecert.exe.* Instead, copy the address for the unzipped eCert program by highlighting the Windows address bar and pressing **Ctrl+C**. Note that this action assumes that you are using the C: drive.
6. In the Start menu search bar, type **cmd** and click **OK**. A command prompt appears.
7. Navigate to the directory that you copied in Step 5. Type **cd** and right-click to paste the directory. Press **Enter**.
8. Type **ECert <merchant_id>** where **<merchant_id>** is your CyberSource merchant ID, and press **Enter**. By default, the eCert application writes the certificate and private key files to the keys\ directory in the directory in which you installed the SDK.

Replacing Expired Keys

Context

When your security keys expire, you must generate new keys and replace the expired ones using this procedure.

1. Download new keys:
   - For the Test environment, download the keys from: http://apps.cybersource.com/library/downloads/CAS/CyberSource_SJC_US.crt
   - For the Production environment, download the keys from: http://apps.cybersource.com/library/downloads/CyberSource_SJC_US.crt
2. Find the currently installed CyberSource Certificate on all machines that send transactions to CyberSource in the environment (Test or Production) that you are updating.
3. Rename the currently installed CyberSource Certificate to **CyberSource_SJC_ US.crt.bak**.
4. Place the newly acquired CyberSource Server Certificate in the same directory as the renamed Server Certificate.

SOAP Security Keys

Before sending requests for CyberSource services using the SOAP API, you must create a security key for your CyberSource merchant account on the Business Center. The SOAP Toolkit API authenticates using a base-64-encoded transaction key represented in string format. You must generate separate security keys for your test environment and your production environment.

Generating SOAP Security Keys

Context

The SOAP API generates a security key you can copy to your clipboard or download as a text file.

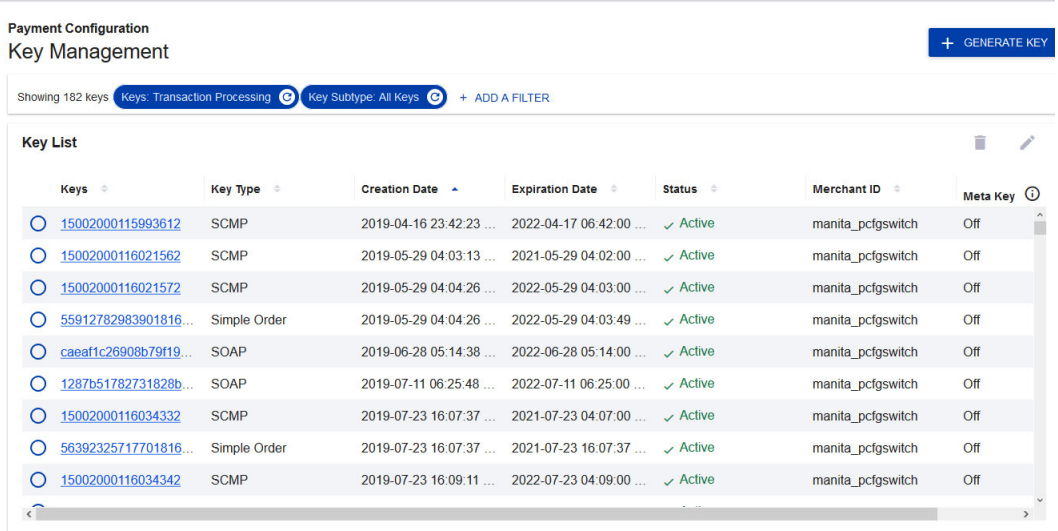
A security key created in the Business Center for the SOAP Toolkit API is valid for three years.

1 Log in to the Business Center.

- Test Environment: https://ebc2test.cybersource.com/ebc2/
- Production Environment: https://ebc2.cybersource.com/ebc2/
- Production Environment in India: https://ebc2.in.cybersource.com/ebc2/

2 From the left navigator pane, choose **Payment Configuration** **> Key Management**.

3 On the Key Management page, in the upper-right, click the **+ GENERATE KEY** button.



4. In the Select a key type dialog, choose **Transaction Processing**. Click **NEXT STEP**.
5. In the Select a key subtype dialog, choose **SOAP**. Click **SUBMIT**.
6. When the authentication key displays, click **DOWNLOAD KEY** to download the key as a text file.
7. Save the text file containing the security key to a secure location.

PGP Security Keys

CyberSource uses PGP encryption for Account Updater response files and Notice of Change (NOC) reports. For information about Account Updater, see the Account Updater User Guide. For information about NOC reports, see Electronic Check Services Using the Simple Order API and Electronic Check Services Using the SCMP API.

A PGP public/private key pair enables you to use encryption to protect credit card data. You exchange the public part of this key pair with CyberSource, which uses the public key to encrypt response files or NOC reports. You use the private part of the key pair to decrypt the response files or NOC reports. Only the private key can decrypt files that are encrypted with the public key.

Creating a PGP Key Pair

You can use any OpenPGP-compliant software to generate PGP keys. The key you generate must be an RSA key. For software solutions, see http://www.pgp.com/, which is part of the Symantec encryption product group. Free OpenPGP solutions are also available:

- Bouncy Castle at http://www.bouncycastle.org/
- GPG4WIN at http://www.gpg4win.org/

CyberSource recommends that you do the following:

- Make the key at least 2048 bits long.
- Store the private key in an encrypted format to protect it from unauthorized use.
- Back up the private key in case of disaster.

WARNING: Place the backup of the private key on removable media and lock it in secure storage.

CyberSource does not receive a copy of your private key and cannot decrypt files that are encrypted with your public key. After you create a public/private key pair, add the public key to the Business Center as described in Adding a PGP Public Key to Your Merchant Profile.

Adding a PGP Public Key to Your Merchant Profile

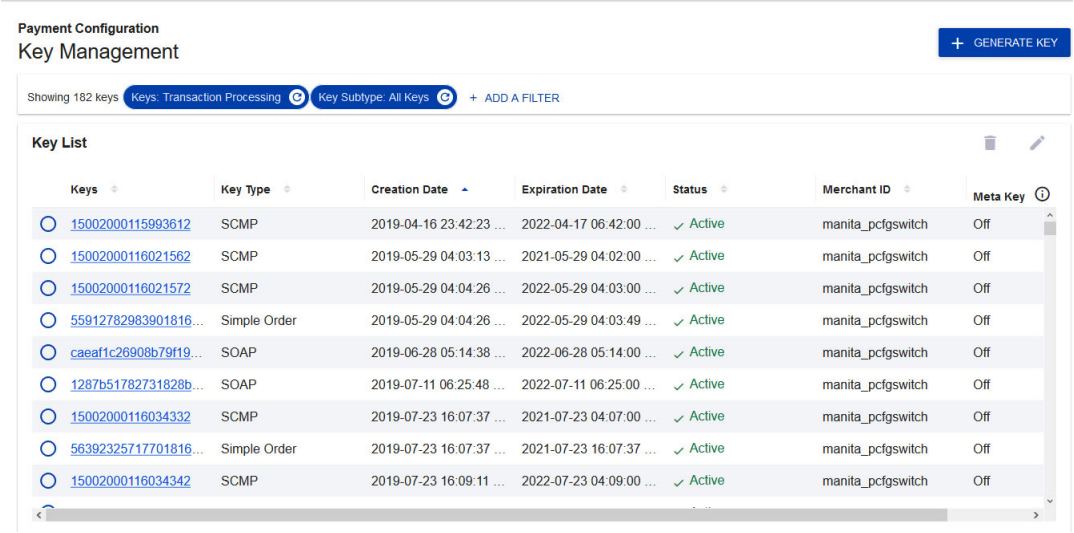
Context

Before you can decrypt a response file or NOC report, you must add the PGP public key that you created to your CyberSource merchant profile in the Business Center. Only the corresponding private key can decrypt files that are encrypted with the public key.

If you do not have administrative privileges, an administrator must grant you Business Center access as described in Granting Business Center User Permissions.

1 After generating a PGP key as discussed in Creating a PGP Key Pair, log in to the Business Center.

2 In the left navigation pane, choose **Payment Configuration** > **Key Management**. The Key Management page appears.



3 On the Key Management page, click the **+Generate Key** button in the upper-right of the Key Management page.

4 In the Select a key type dialog, choose **PGP Key**.

5 Click **Next Step**.

6 In the Key Configuration dialog, copy the ASCII string of the PGP key into the **PGP Key Value** field. Here is an example of an ASCII string for a PGP key:

mQENBEnUeKQBCADI97dqBLOmIehGIuNWr08deuj6ym+CdrJ/IcugVqv1Od7iypT+
pu8zU2mEFTXWMLmf363KU8yNhbR3iSn5DKwpT/XLQ/SmaKOMv/ZZ2KoHbz5zGdd/
5nA/yIS3YvcACq+ZPpYS0as4LpJ4B6dnDuLroxMNjI+cxdXvJ7Rzt4Rqg+ro1KD3
URxqMa0wQbxm8R07k6wsNV1EJuPJ9N5ogYuPKdGyJ3TPQxdQtiqsRFF/KeuwNPk5
BPeOKnSbc4GPyiIno1AA3pwdLgw4HIZ3POWq6Zu5jGOJiub8C1qtBUI0Hend73jh
kQmLylz17C5NdjfpCZSsxhee36lGsOALM2pXABEBAAG0I2ljYV90ZXN0XzEgPGds
bG95ZEBjeWJlcnNvdXJjZS5jb20+iQE2BBMBAgAgBQJJ1HikAhsPBgsJCAcDAgQV
AggDBBYCAwECHgECF4AACgkQc8du5ok+OYj3PAf/d3zwP+cBaJUMp61foljMsCF6
JNpkCiI9A3gkkf6Z2YgVhfH1OXf1JsN3jDOBEkt24um5HfhmhsDy+x4VAQyEuzcN
Mst5FQBfLUOsy1tTz+RgDGlKUtSsbzJ9puURfRiyN0pqWoHmR2mTJq8puziOSNj4

WAaBq9Jq8o1R35xvrKkle/JGT24jTSwFDGcLIwRxndnutlvaftbkirVrCpRs5Cj/
u4HDh/tXmRKmKrGKOEhn2l1uYX2aLsSJnnlGoY7W+wYsJImw4j3EOa0WtPA3mO41
SfCYIohI4gkPH4eC/IQcoMkZZ1kV+HiA1wIimWez/YuqSsmPBubELB9VzxMLLA==
=y2uP

IMPORTANT: Do not copy the header and footer when you copy the string. Here is an example of a header:

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP 8.1 - not licensed for commercial use:
www.pgp.com

Here is an example of a footer:

```
-----END PGP PUBLIC KEY BLOCK-----
```

7 Click **Submit**.

8 Refresh the screen to view your new key. If you have many security keys, you may need to use the Keys filter at the top of the Key List to filter the screen to only show PGP keys.

9 In the Key List, click the **Active** button next to your new key.

10 Click **Activate**.

Granting Business Center User Permissions

Context

A user account in the Business Center requires certain permissions to work with PGP keys and the Account Updater request files and reports.

1 Log in to the Business Center.

2 In the left navigation pane, choose **Account Management**  **> Roles**.

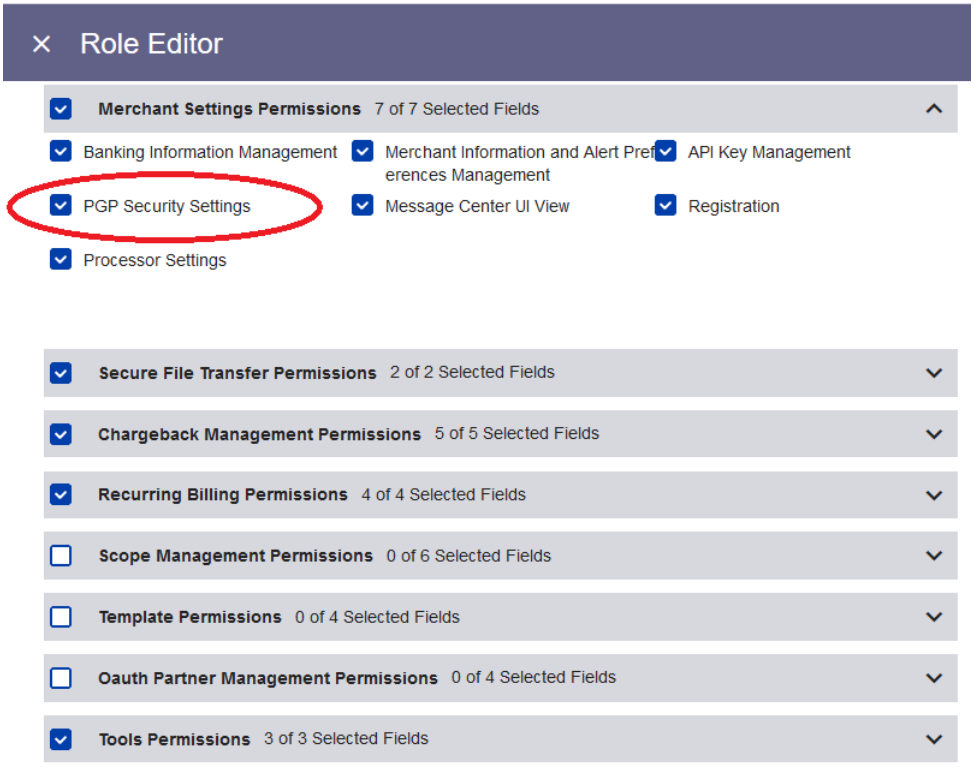
3 Choose the role assigned to the user account that needs to work with PGP keys and click on the **Edit**  icon.

4 In the Role Editor, select the following permissions:

   a Under Credit Card Account Updater Permissions, choose **View Status**. This option enables the user to view the status of uploaded Account Updater request files and NOC reports.

   b Under Merchant Settings Permissions, choose **PGP Security Settings**. This option gives the user permission to upload, activate, and deactivate encryption keys.

c Under Reporting Permissions, choose **Report Download**. This option gives the user permission to download Account Updater response files and NOC reports.



5 At the bottom of the Role Editor, click **Save**.