Agency Guide to Access Control

August 21, 2023

REVENUE COLLECTIONS MANAGEMENT
BUREAU OF THE FISCAL SERVICE

This version of the *Agency Guide to Access Contro*l supersedes all previous versions.

Revision History

Date	Author	Description
July 17, 2007	Maureen Redig and Brian Asquith FRB Cleveland	Initial version.
July 26, 2007	Maureen Redig and Brian Asquith FRB Cleveland	Revised section 4.3 (accounts locked for 15 minutes).
August 1, 2007	Douglas Kirchgesler FRB Cleveland	Formatting and layout revisions
January 4, 2008	Douglas Kirchgesler FRB Cleveland	Updated for Pay.gov 3.8.
June 2, 2008	Douglas Kirchgesler FRB Cleveland	Updated for Pay.gov 4.0 (added section 2.2; updated sections 1.1, 3.1, and 3.3).
September 15, 2008	Douglas Kirchgesler FRB Cleveland	Updated for Pay.gov 4.1 (added section 2.2; updated table 1 and sections 4.2.1 and 4.2.2).
November 12, 2008	Douglas Kirchgesler FRB Cleveland	Updated for Pay.gov 4.2 (minor typographical revisions).
February 5, 2009	Douglas Kirchgesler FRB Cleveland	Updated for Pay.gov 4.3 (updated section 2.1.2, section 5.1, and table 1).
August 3, 2009	Douglas Kirchgesler FRB Cleveland	Minor layout revisions; discontinued Pay.gov version number on document; updated table 1.
August 6, 2009	Douglas Kirchgesler FRB Cleveland	Updated section 2.1.2.
October 2, 2009	Douglas Kirchgesler FRB Cleveland	Updated sections 1.1, 2.2, and 3.3.
November 23, 2009	Douglas Kirchgesler FRB Cleveland	Updated for Pay.gov 4.4 (updated table 1 and section 2.1.2).
February 23, 2010	Douglas Kirchgesler FRB Cleveland	Updated for Pay.gov 4.5 (updated sections 2.1.4 and 2.3).
March 18, 2010	Douglas Kirchgesler FRB Cleveland	Updated sections 2.2, 3.5, 4.2.1, 4.2.2, and 5.1.
April 21, 2010	Douglas Kirchgesler FRB Cleveland	Updated for Pay.gov 4.6 (minor formatting changes).
August 10, 2010	Douglas Kirchgesler FRB Cleveland	Updated for Pay.gov 4.7 (updated sections 1 and 2.2; removed section 2.1.5; revised Pay.gov logo; replaced "Pay.gov Information Security" with "Pay.gov Application Security throughout).

Date	Author	Description
October 7, 2010	Douglas Kirchgesler FRB Cleveland	Updated for Pay.gov 4.8 (updated table 1).
December 7, 2010	Douglas Kirchgesler FRB Cleveland	Reviewed for Pay.gov 4.9 (no changes).
June 14, 2011	Walter Rowinsky FRB Cleveland	Updated for Pay.gov 5.0 (section 2.1. table 1).
December 19, 2011	Walter Rowinsky FRB Cleveland	Updated for Pay.gov 5.1 (section 3.3).
August 4, 2012	Walter Rowinsky FRB Cleveland	Reviewed for Pay.gov 5.2 (no changes).
December 31, 2012	Walter Rowinsky FRB Cleveland	Reviewed for CA$HLINK II shutdown (no changes).
February 19, 2013	Walter Rowinsky FRB Cleveland	Reviewed for Pay.gov 5.3 (no changes).
March 18, 2013	Walter Rowinsky FRB Cleveland	Updated for Pay.gov 5.3 second test cycle (replaced Access Control Worksheet with Access Request Worksheet).
May 1, 2013	Walter Rowinsky FRB Cleveland	No Pay.gov 5.4 release (merged with Pay.gov 5.3).
May 1, 2013	Walter Rowinsky FRB Cleveland	Updated for Pay.gov 5.5 (replaced references to FMS with Bureau of the Fiscal Service; updated table 1; sections 1.1, 2.1.4, 2.2, 3.3.4, 4.2,).
June 10, 2013	Walter Rowinsky FRB Cleveland	Reviewed for Pay.gov 5.6 (no changes).
September 20, 2013	Walter Rowinsky FRB Cleveland	Reviewed for Pay.gov 5.7 (no changes).
February 8, 2014	Walter Rowinsky FRB Cleveland	Reviewed for Pay.gov 5.8 (updated section 2.2).
April 21, 2014`	Walter Rowinsky FRB Cleveland	Reviewed for Pay.gov 5.9 (no changes).
June 2, 2014	Walter Rowinsky FRB Cleveland	Updated for Pay.gov 6.0 (updated sections 1, 2.1, 2.1.1, 2.1.2, 3.3, 3.3.2).
August 11, 2014	Walter Rowinsky FRB Cleveland	Reviewed for Pay.gov 6.1 (no changes).
October 3, 2014	Walter Rowinsky FRB Cleveland	Updated for Pay.gov 6.2 (updated section 1.1, table 1).
December 3, 2014	Walter Rowinsky FRB Cleveland	Updated for Pay.gov 6.3 (updated sections 1.1, 2.1.3, and table 1).
March 15, 2015	Walter Rowinsky FRB Cleveland	Updated for Pay.gov 6.4 (updated sections 1.1, 2, 2.1, 2.1.1, 2.1.2, and table 1; corrected typos).
June 15, 2015	Walter Rowinsky FRB Cleveland	Updated for Pay.gov 6.5 (updated table 1 and section 2.1.3).

Date	Author	Description
September 21, 2015	Walter Rowinsky FRB Cleveland	Reviewed for Pay.gov 6.6 (no changes).
December 1, 2015	Walter Rowinsky FRB Cleveland	Reviewed for Pay.gov 6.7 (no changes).
March 12, 2016	Walter Rowinsky FRB Cleveland	Updated for Pay.gov 6.8 (corrected typos and formatting).
June 13, 2016	Walter Rowinsky FRB Cleveland	Updated for Pay.gov 6.9 (most sections updated).
August 1, 2016	Walter Rowinsky FRB Cleveland	Corrected typos.
September 18, 2016	Walter Rowinsky FRB Cleveland	Updated for Pay.gov 6.10 (updated section 3.3).
December 17, 2016	Walter Rowinsky FRB Cleveland	Updated for Pay.gov 6.11 (updated sections 7.3 and 7.8)
April 17, 2017	Walter Rowinsky FRB Cleveland	Updated for Pay.gov 7.0 (updated section 4.6).
July 17, 2017	Walter Rowinsky FRB Cleveland	Reviewed for Pay.gov 7.1 (no changes).
October 16, 2017	Walter Rowinsky FRB Cleveland	Updated for Pay.gov 7.2 (updated section 6.2).
January 26, 2018	Walter Rowinsky FRB Cleveland	Updated for Pay.gov 7.3 (corrected typos in the table in section 7.8).
July 1, 2019	Walter Rowinsky FRB Cleveland	Updated for Pay.gov 7.9 (updated website URLs; removed references to CCP; updated section 7).
February 14, 2020	Walter Rowinsky FRB Cleveland	Updated section 2.5; deleted section 7.6 – CCP; added new section 7.8.
February 1, 2021	Walter Rowinsky FRB Cleveland	Updated for Pay.gov 7.15 (added new sections 4.9 and 7.9; updated section 7.1).
October 10, 2022	Walter Rowinsky FRB Cleveland	Updated for Pay.gov 8.0 (new sections 2.6.3,4.10, 6.4, and 7.4; updated sections 2.3.4, 2.5, 2.6.1, 6, and 8.1.1).
March 14, 2023	Walter Rowinsky FRB Cleveland	Updated for Pay.gov 8.1 (added section 2.6.4).
August 21, 2023	Walter Rowinsky FRB Cleveland	Updated for Pay.gov 8.3 (updated sections 2.3.4, 2.6.4, 3.1, 3.2, 3.3, 4, 6.1, 7.7; added new section 7.8).

Table of Contents

1 Introduction

This document provides agency users who have been designated as Pay.gov security contacts a basic understanding of the security used in Pay.gov. It also provides:

- The processes for assigning and/or changing Pay.gov security contacts
- The process for requesting access to the Pay.gov test and production systems
- Access control for agency users
- Access control for agency customers whose accounts on Pay.gov's public website is set up by an agency

1.1 Related Documents

Related and supplemental agency guides, and reference manuals are available on the Pay.gov Agency Documentation site at https://qa.pay.gov/agencydocs/ or by request from Pay.gov Customer Support.

2 Overview of Access Control

2.1 Access

Access defines:

- The services and parts of Pay.gov's systems a user, customer, or agency system can interact with
- The specific agency collection application(s) or resource data a user or customer can see
- The functions a user (agency or customer) can perform on the cash flow application's or resource's transaction data

> ***Note:*** For this explanation of access, a resource is a billing account number (BAN). Bills are created for a BAN and one or more customers are associated with the BAN. All RBU role users associated users with the BAN can access all bills created for the same the BAN.

An agency user or customer can have access to multiple applications.

2.2 Roles

Roles are assigned at the application level to a specific user.

For example, if an agency user has access to two applications, their roles are assigned separately to each application.

Roles define what functions the user can perform on Pay.gov for the specified application. Users can be assigned multiple roles.

Roles are grouped by category: public roles, agency user roles, resource user roles, and system roles. Some roles are automatically assigned the permissions for other roles or can be assigned to accounts that include other roles.

Roles are described in sections 3, 4, 5 and 6.

2.2.1 Users can have multiple roles

Agencies can assign more than one role to a user. For example, an agency user can have both a role that allows them to use the Collection Control Panel and a role that allows them to view reports. They then can perform all the functions permitted by both roles.

Many roles also automatically grant the PGE role permissions.

2.3 Role Permission Levels

2.3.1 Public Roles

- Allow access to Pay.gov's public website only.
- Allow anyone visiting the public website to use and make payments for any publicly-available form and to access some bills without signing in

- Access to private agency forms, some bills, and transaction histories requires the user be assigned specific roles for the application that has the private form or bill.
- Some roles may allow reassigning forms to another user if the application allows.

2.3.2 Agency User Roles

- Allow access to Pay.gov's myagency website
- May include an automatically assigned public role
- The agency user must have a Pay.gov account (requested by the agency)
- The agency user must sign in
- Define which functions agency users will see on the myagency Agency Collections website

> ***Note:*** Access to agency applications and information varies according to permissions the agency requests for each agency user's role.

2.3.3 Resource User Roles

- Allow access to the bills created for a BAN on Pay.gov's public website
- May be assigned to both customers and agency users

2.3.4 System Roles

- Allow access to Pay.gov web services including TCS Services, Collections API, and Activity File download.
- Allow automated upload and download of data for some Pay.gov services and functions
- Examples include machine accounts and the role associated with Collections API authentication

2.4 Control

Your agency controls access and roles by submitting the Access Request Worksheet (ARW) for the Pay.gov service used by your application(s) to the email address on the instruction page.

The ARW is completed and submitted by your agency's Pay.gov Security Contact (see section 8.1).

An ARW

- Identifies the Pay.gov environment access is to be granted to. Submit separate ARWs for Production or Test
- Identifies the application(s) access will be granted to
- Allows you to create application new users
- Allows you to assign roles to new users and exiting users
- Allows you to delete roles for existing users
- Allows you to delete users by application

2.5 Access Request Worksheets

> ***Important:*** You must use the specific ARW for the Pay.gov service used for your collection application.
>
> ***Note***: The roles available in an ARW vary according to the Pay.gov service.

ARW's are available on Pay.gov's Agency Documentation website at https://qa.pay.gov/agencydocs/html/acforms.html:

Access Request for Bills — create and delete users, grant, assign or remove user roles, create BANs, assign users to BANs for applications using the legacy Billing Service.

Access Request for eBilling — create and delete users, assign or delete user roles for applications using the eBilling Service and eBilling Online.

Access Request for Forms — create and delete users, assign or delete user roles for applications using the Pay.gov Hosted Forms Service, including public, public hidden and private forms.

Authorization User Account Access Request Worksheet — create and delete users, assign or delete user roles for applications using:

- Collections API
- TCS Web Services
- eBilling Web Services (eBillingService, AccessCodeService)
- eBilling Online Application and eBilling Online Web Service
- ACH Credit Web Service

Access Request for Machine ID — create and delete users, assign or delete roles used for the automated processes to upload billing files for the Billing Service and to download activity files. Activity file descriptions are found in the *Agency Guide to the Reporting Service*.

2.6 Other Access Controls

2.6.1 Security Certificates

Web Services — For your system to communicate with any Pay.gov web service, new applications must request and install an Entrust Security Certificate issued by the Treasury Operational Certificate Authority (TOCA).

The communication certificate request is at https://qa.pay.gov/agencydocs/html/acforms.html.

For download and installation instructions, request the *Web Services SSL Certificate Support Guide* at https://qa.pay.gov/agencydocs/.

> ***Note:*** If you are already using a security certificate to access a Pay.gov web service, you do not need to install another one. Your existing certificate may be used to communicate with any Pay.gov web service used by your new cash flow

applications. See the certificate access request worksheet in section 2.5, and roles and permissions table in section 7.8.

2.6.2 Access to Public Hidden Forms

Public hidden forms are not directly available on Pay.gov's public website. Your agency must provide the hidden form URL (link) to any users that need access. No other access control is required.

2.6.3 Collections API Authentication Credentials

- Allow access to Collections API.
- Allow agencies to submit transactions to Collections API.
- Agencies will be notified by email when credentials are available. Pay.gov sends a one-time URL to the agency to be used when downloading the credentials. The URL is available for only a six hour period. You must down load your API credential within the six hours. After the six hour period the URL is no longer valid.
- Credentials expire after 13 months, and new ones need to be requested.

2.6.4 Pay.gov Account and Sign In

Users must sign in to access their Pay.gov account on the public website or the Agency Collections (myagency) website. Using one of the single sign on methods below is required for all users.

- On the public website customers and agency users must connect their account to a Login.gov or ID.me sign in.
- On the Agency Collections (myagency) website, agency users must sign in using their PIV/CAC employee ID. (A small number of agencies may not require use of a PIV/CAC ID. Contact your Pay.gov Agency Implementation Specialist if an exemption or instructions are required.)
- Agency users with new accounts must first sign in using the Pay.gov username and password given to them and then associate their Agency Collections account with their PIV/CAC.

Note: Only one account can be associated with Login.gov or ID.me. Login.gov and ID.me accept only one email address. Users having multiple accounts that use the same email address should contact Pay.gov Customer Support for help.

3 Public Roles

Public level roles can only access Pay.gov's public user interface but might be assigned to agency users to allow them access to both the public and agency websites.

3.1 Public User

A public user is any customer who is not enrolled with Pay.gov. (does not have a Pay.gov account) They can access any form or function available to all users visiting the public website.

Public user permissions are very limited. A public user may only

- View public reports
- View and submit payments for public forms
- View and submit payments for hidden public forms if they have been given the URL by an agency
- View and submit payments for public ebills if they have the required access information

This role requires no access request from an agency.

3.2 Pay.gov Enrolled User (PGE)

The PGE role is automatically assigned to any enrolled user, whether they create a Pay.gov account or are have an account created for them by an agency.

By itself, the PGE role can only access Pay.gov's public website, but the user must sign n using ID.me or Login.gov to take advantage of the PGE's Pay.gov account functions.

In addition to the activities allowed for a Public user, PGE users

- Have and can modify a user profile
- Can view and submit private forms they have permission to access
- Can save their own submitted forms
- Can make recurring payments when allowed by the collection application
- Can view and pay public ebills
- Can view and pay private ebills (if enrolled by an agency)
- Can view and pay private forms (if enrolled by an agency)
- Can view their payment history
- Can reset their password.

In addition to being a role in itself, the PGE role permissions are automatically assigned to agency users with other roles (it does not have to be requested separately). For example, if a user is assigned the ROA role they automatically receive the PGE permissions as well.

An access request (ARW) is only required if the agency is enrolling the customer; for example, to grant them permission to view a private form and when creating AFL or ARW users see section 3.3.). Pay.gov creates the username and a temporary

password for users enrolled by an agency. The user then must associate their new account with ID.me or Login.gov.

3.3 Application Forms Limited (AFL) and Application Forms Full (AFF)

> ***Important!*** Separate AFL and AFF accounts cannot have the same email address. Users should contact Pay,gov Customer support for help.

Typically, the AFL and AFF roles are assigned to organization customers (such as a business) who must use an agency's private form and who require that entering data be separated from submitting the form and making any associated payment.

The AFL user can enter the data but not submit the form. The form must be reassigned to an AFF user if it is to be submitted and any associated payment made.

For example, a business may require a three-step process to submit a form. The form is opened and completed by an AFL user who reassigns it to a second AFL user. The second AFL user reviews it and reassigns it to an AFF user. The AFF user submits the form and makes the associated payment.

Each time the form is reassigned it is removed from the Pay.gov account of the user reassigning it and moved to next user's account. It is no longer available to the user who reassigned it.

> ***Important!*** When assigning an AFL role to a user, a corresponding AFF role must be created or be already available.

Both roles are also automatically granted PGE role permissions, and so can perform those functions in addition to the AFL or AFF functions.

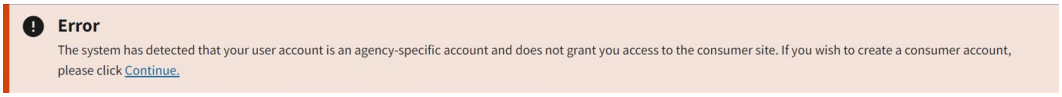
Your agency's Pay.gov Security Contact must enroll these customers and grant them the appropriate role by submitting the appropriate ARW.

3.3.1 Account Associated with ID.me or Login.gov Required

AFL and AFF users must create an account on Pay.gov's public site and associate it with ID.me or Login.gov sign in. The account can then be assigned the correct role through the Access Request Worksheet process.

AFL and AFF users who had the role prior to the ID.me/Login.gov requirement also need to create an account on Pay.gov's Public website. They may see an error message stating that they have an agency-specific account and they must click Continue to create a new Pay.gov account.

Figure 1: AFL/AFF error message



3.3.2 AFL

By itself the AFL role has limited permissions. AFL users can

- View a private form
- Enter data
- Save the form
- Edit a saved form
- Reassign the form to another AFL or AFF user

AFL users cannot submit the private form or make an associated payment.

3.3.3 AFF

The AFF role has all the permissions of the AFL role plus the ability to submit forms and make payments. AFF users can

- View a private form
- Enter data
- Save the form
- Edit a saved form
- Reassign the form to another AFL or AFF user
- Submit the form
- Submit an ACH debit or plastic card payment
- Cancel an ACH debit payment
- Submit a digital wallet payment if the method is enabled for the application
- View/edit saved and view owned form instances
- View saved forms and completed transactions in their Pay.gov account

For example, if permitted by the organization, an AFF user could perform the entire process of opening a private form, entering data, submitting it, and making the associated payment. Or they could open a form, save it, reassign it to an AFL user for completion and then submit the form when it is reassigned back to them.

Typically, however, an AFF user would receive a form reassigned to them by an AFL user and then submit it and make the payment.

The role is also automatically granted PGE role permissions.

4 Agency User Roles

Agency user roles are assigned to users who perform specific functions for an application, such as viewing reports or entering payment information for a customer. Multiple roles can be assigned to allow an agency user to perform a range of functions.

All agency user roles have PGE role permissions, limited to Pay.gov's Agency Collections website, which means they are required to sign in and are able to manage their account profile information. When an agency user role is created, Pay.gov creates the username and temporary password. Then the agency user must associate the account with their PIV/CAC card.

> ***Note:*** Some agency users, such as customer service, will need both agency user roles and a public user role so that they have access to both websites.

4.1 Report Office Analyst (ROA)

The ROA role is assigned to agency users who must work with non-public reports and activity files. ROA users can view most of the non-public reports for any application they have access to.

It is also assigned to system-level accounts designated as machine general accounts (MGA), which can be set up to automatically schedule the download of activity files and the upload of billing files. An account with the MGA role must be also created to access Activity Files via the Activity File Service or the Activity File Servlet. Refer to section 6.1 for more information about machine accounts.

4.2 Application Customer Service (ACS)

The ACS role is assigned to agency users responsible for providing customer service support for one or more designated agency applications. Agency users with this role should also be assigned a public user role for their applications so they can view private forms on Pay.gov's public website.

ACS users can

- Search for and view transactions, forms, and bills submitted by others
- Access to most non-public reports, including the enrolled user report, which lists users assigned to the application
- view users and their assigned roles

ACS users cannot enter data, submit forms, or enter payment information.

4.3 Bill Generator (BIG) and Bill Access Generator (BAG) Roles

The BIG and BAG roles are assigned to agency users who access the eBilling Online Application and the eBilling Online Web Service.

Collections applications that use the eBilling Online Application require both roles. Security is enhanced by separating the functions required to issue an ebill.

The BAG users can only create ebills and billing accounts. BAG users manage customer access to the ebills.

4.3.1 Bill Generator (BIG)

The BIG role can only access the eBilling Online Application. BIG users can

- Create bills
- Cancel bills
- Create billing accounts (BANs)
- Upload batch files to create multiple ebills

A corresponding BAG role user is required to issue an ebill.

4.3.2 Bill Access Generator (BAG)

The BAG role can only access the eBilling Online Application. BAG users can

- Create bill access codes
- Create customer billing accounts (BANs)
- Create payers for billing accounts
- Monitor access code use
- Resend access codes to payers when needed
- Upload batch files to create multiple access codes

A corresponding BIG role is required to create an ebill.

4.4 Company Profile Administrator (CPA)

The CPA role is assigned to agency users who create and manage company profiles for their application.

CPA users can

- Create, modify, and delete profiles
- Assign users to one or more company profiles
- View and use a limited number of reports: Company Profile Access Query, Company Profile Scope Values Query,

A company profile is a set of values created for an organization, which is configured for a collection application and stored on Pay.gov. A profile can automatically populate certain form fields when a Pay.gov account (user) that has been associated with the profile opens and submits the form.

See the *Agency Guide to Company Profiles* for additional information.

4.5 Collections Operator Sale (COS)

The COS role is assigned to agency users who submit transactions through the Create Transactions Service and for viewing Pay.gov reports on the Agency Collections (myagency) website.

COS users can

- Search for and view previously submitted transactions

- Submit plastic card authorization requests
- Submit plastic card sales
- Force previously authorized plastic card transactions
- Submit ACH debit transactions
- Submit ACH debit prenotifications
- Search for and view previously submitted transactions
- View summary and detailed transaction reports and activity files
- Enroll customers in automatic bill payment
- Edit customers' enrollment in automatic bill payment

This role may be assigned in conjunction with the COE role; however, you should consider separation of duty requirements before doing so.

4.6 Collections Operator Exception (COE)

The COE role is assigned to agency users who use the Create Transactions service to submit and manage transactions.

COE users can:

- Process plastic card refunds and voids
- Process ACH cancellations
- Edit ACH debits
- Request digital wallet refunds when allowed by the payment service

Users with the COE role may also perform refunds without a Pay.gov tracking ID (stand-alone refunds) if the application has been authorized to do so by the Bureau of the Fiscal Service and the option is enabled in Pay.gov.

This role may be assigned in conjunction with the COS role; however, you should consider separation of duty requirements before doing so.

4.7 Payer Profile Administrator (PPA)

The PPA role is assigned to agency users who create, manage, and verify payer profiles for their application(s).

A payer profile is a set of values created for a payer with a Pay.gov account and an ACH account. It is associated with an application and stored on Pay.gov that can automatically populate certain form fields (payment account information, for example). The fields are populated when a user with a Pay.gov account associated with the profile opens or submits the form.

PPA users can

- Create, manage, and view payer profiles

4.8 Payer Report Administrator (PRA)

The PRA role is assigned to agency users who need to view payer profile reports for their agency application(s).

PRA users can

- View and use the Notification of Change Search Query
- View reports only available to agencies using payer profiles
  - Payer Profile Audit Log Search Query
  - Payer Profile Collections Search Query
  - Payer Profile Search Query

4.9 Security User (SEC)

The SEC role can be assigned to agency users who will conduct the annual review and recertification of users (User Access Recertification) through the My Agency (myagency) website.

SEC users can

- Sign in to the myagency website
- Review and request recertification of agency users

4.10 Collections API (API)

The API role is assigned to cash flow applications using the Collections API.

API applications can

- Submit transactions
- Cancel transactions
- Submit ACH pre-notifications

5 Resource Roles

Resource roles provide permissions that could span multiple agency applications. Pay.gov has only one resource role.

5.1 Resource BAN User (RBU)

The RBU role is assigned to agency billing customers.

Billing Account Numbers (BANs) are used to determine which customers have access to a bill. An agency creates a BAN, which can be assigned to one or more bills created for any of its applications(s) using Pay.gov's eBilling service, eBilling Online, or legacy Billing service.

When sign in is required to access a bill for the first time (private ebill), Pay.gov automatically assigns the RBU role to the customer's account after they successfully sign in and access the bill. From then on, all bills assigned the BAN appear in the customers My Account – My Bills lists.

If sign in is not required to access an ebill (public ebill) the RBU role is not assigned to the customer's Pay.gov account.

RBU users can

- View and pay bills they have been given access to
- View pending and completed bills
- Cancel some bill payments

See the *Agency Guide to the eBilling Service*, the *Agency Guide to eBilling Online* and the public website's Online Help for more information on BANs and bills.

6 System Roles

System roles grant permission to access Pay.gov's systems for automated upload or download, or for applications to communicate with Pay.gov's web services.

6.1 Machine General Account (MGA)

Machine accounts are used as part of the automated processes to

- Upload billing files (legacy Billing service)
- Download activity files (system-to-system, using the Activity File Service, or using the Activity File Servlet).

A single machine account may be used for all applications within an agency, or the agency may request a machine account may request a separate MGA for each application.

> ***Note:*** A separate account with the MGA role is required to download using the Activity File Service or the Activity File Servlet. Contact Pay.gov Customer Support for information.

However, multiple machine accounts are not generally needed because the report generated for each activity file will contain the information for all activity files by agency application. You must indicate on the access request worksheet if a separate machine account will be needed for each application.

The MGA is assigned to the agency user who will be managing that account, and the ROA role and PGE permissions are automatically assigned to the MGA.

If the individual who is assigned ownership of the machine account no longer needs access, an agency's Pay.gov security contact must fill out and submit the *Access Request Worksheet to Manage MGA Machine IDs* to remove and reassign ownership.

Machine account passwords do not expire. The agency security contact is responsible for ensuring the password for the machine account is changed at least annually or whenever individuals no longer need to know it, such as employee separation or job change.

> ***Important!*** An account with the MGA role is required to access Activity Files when using the Activity File Service, the Activity File Servlet, or system-to-system download. MGA accounts cannot be used to sign in to Pay.gov's Agency Collections (myagency) website.

6.2 Certificate User (CRT)

The Certificate User role (CRT) grants permission for an authorized-agency-system to access one or more of the following Pay.gov services:

- The selected Trusted Collections Web Service (TCS)
- The eBilling and the Access Code services
- The eBilling Online Web Service (not the eBilling Online Application)

- The ACH Credit Web Service
- Pay.gov Hosted Collection Pages

A security certificate is required for your agency system to communicate with Pay.gov's system.

1. An application using one of these services must be created.
2. After the application has been configured, your agency security contact must submit an Access Request for TCS, CCP, and OCI (ARW) to create the CRT role for the service created.
3. Your agency must obtain a security certificate from the Treasury Operational Certificate Authority (TOCA), which will be linked to the Pay.gov CRT account and authorizes your agency system to communicate with the appropriate services on Pay.gov's system. See the *Web Services SSL Certificate Support Guide* for instruction on how to obtain a certificate.

> ***Note:*** If your agency already has a security certificate used for a TCS web service it may also be used for any Pay.gov service that requires a certificate. However, your agency security contacts must amend your existing ARW (or submit a new one) to grant application access to the additional services.

6.3 Trusted Collection Service (TCS)

In addition to a certificate user role (CRT), a TCS role is assigned to cash flow applications accessing TCS services.

6.4 Collections API

Cash flow applications using the Collections API are assigned the API role.

7 Roles and Permissions Tables

> ***Note:*** Roles marked with an asterisk (*) in the tables below also have PGE permissions.

7.1 Public Website, Payments, Forms and myagency Website

Permissions Public Website, Payments, Forms and Agency Website	Public	PGE	AFL*	AFF*	ROA*	ACS*	BIG*	BAG*	CPA*	COS*	COE*	PPA*	PRA*	RBU*	MGA	CRT	SEC
Public Website, Payments and Forms																	
Search for Forms	X	X	X	X		X											
Submit Plastic Card Payment	X	X		X										X			
Submit payment ACH debit	X	X		X										X			
Cancel ACH Debit		X		X										X			
Submit Digital Wallet Payment	X	X		X										X			
View and Submit Public Form	X	X															
Save Public Form	X	X															
View Private Form		X	X	X													
Submit Private Form		X	X	X													
Reassign Private Forms			X	X													
View public and private non-owned forms						X											
View saved forms		X	X	X													
Update own user profile		X	X	X										X			
myagency Website																	
Update own user profile					X	X	X	X	X	X	X	X	X				X

> ***Note:*** Sign in credentials (email address and password can only be updated on Login.gov and ID.me.

7.2 Agency Customer Service

Permissions Customer Service at Agency	Public	PGE	AFL*	AFF*	ROA*	ACS*	BIG*	BAG*	CPA*	COS*	COE*	PPA*	PRA*	RBU*	MGA	CRT
Access Agency Collections (myagency) website							X	X		X	X					
View role summaries						X										
Create Plastic Card Sales transactions										X						
Create Plastic Card Force transactions										X						
Create Plastic Card Authorizations										X						
Refund Plastic Card transactions											X					
Void Plastic Card Transactions											X					
Create ACH Debit transactions																
Edit ACH Debit transactions																
Cancel ACH Debit transactions											X					
Request PayPal transaction refunds											X					
Enroll customers in Automatic Bill Payment										X						
Edit Automatic Bill Payments										X						
Cancel Automatic Bill Payments										X						
Pay a Form on Agency Collections (myagency) website										X						
Access online reports (see reports table)						X				X	X					
Access activity files (see reports table)						X										
Search transaction via Transaction Search						X				X	X					
View transaction details										X						
View non-owned reports						X										
View non-owned bills						X										

7.3 Bills, eBilling Services, eBilling Online

7.3.1 Bills

Permissions Bills	Public	PGE	AFL*	AFF*	ROA*	ACS*	BIG*	BAG*	CPA*	COS*	COE*	PPA*	PRA*	RBU*	MGA	CRT
View, edit, save, and submit bill														X		
View pending and completed (submitted)bills														X		
View non-owned bills						X										

7.3.2 eBilling Services

Permissions eBilling Services	Public	PGE	AFL*	AFF*	ROA*	ACS*	BIG*	BAG*	CPA*	COS*	COE*	PPA*	PRA*	RBU*	MGA	CRT
Access eBilling Services																X
Create BAN, create, or cancel bill																X
Create access code, resend, and cancel access code																X
Resend access code																X
Cancel access code																X

7.3.3 eBilling Online Application (Agency Collections / My Agency Website)

Permissions eBilling Online Application	Public	PGE	AFL*	AFF*	ROA*	ACS*	BIG*	BAG*	CPA*	COS*	COE*	PPA*	PRA*	RBU*	MGA	CRT
Access eBilling Online Application							X	X								
Create bill							X									
Create, view, and edit custom bill content (logo, comments)							X									
Create/edit custom bill data							X									
Create and view bill line items							X									
View bill list							X									
View bills and bill details							X									
Edit bill							X									

Permissions eBilling Online Application	Public	PGE	AFL*	AFF*	ROA*	ACS*	BIG*	BAG*	CPA*	COS*	COE*	PPA*	PRA*	RBU*	MGA	CRT
Cancel bill							X									
Batch upload ebills							X									
Copy and edit bill							X									
Cancel online bills																
View bill status							X									
Search and view online bill payments							X									
Cancel automatic bill payment							X	X								
Create customers							X									
Batch upload customers							X									
Search & view customers							X									
Create BAN							X									
View BAN list							X	X								
Create and manage bill payers							X									
View bill payer list							X	X								
Attach files							X									
Create BAN access code								X								
Send access code								X								
Resend access code								X								
Cancel access code								X								
View access code email							X	X								
Update access code email							X									
Export formatted report data							X									

7.3.4 eBilling Online Web Service

Permissions eBilling Online Web Service	Public	PGE	AFL*	AFF*	ROA*	ACS*	BIG*	BAG*	CPA*	COS*	COE*	PPA*	PRA*	RBU*	MGA	CRT
Upload bill and access code data																X
Upload customer data																X

Important! Agency users who need to view and edit bills, or who will create or upload custom bill content should be assigned the BIL and BAG roles for the associated eBilling Online Application. See section 7.5.3.

7.3.5 eBilling Service (Legacy)

Permissions Legacy eBilling Service	Public	PGE	AFL*	AFF*	ROA*	ACS*	BIG*	BAG*	CPA*	COS*	COE*	PPA*	PRA*	RBU*	MGA	CRT
Upload bill data to the legacy Billing service															X	

7.4 Collections API

Permissions Legacy eBilling Service	Public	PGE	AFL*	AFF*	ROA*	ACS*	BIG*	BAG*	CPA*	COS*	COE*	PPA*	PRA*	RBU*	MGA	CRT	API
Access Collections API																	X

> ***Note:*** API role is assigned to the cash flow application. Authentication credentials and signature are required for each transaction.

7.5 Payer Profile (Agency Collections / My Agency Website)

Permissions Payer Profile	Public	PGE	AFL*	AFF*	ROA*	ACS*	BIG*	BAG*	CPA*	COS*	COE*	PPA*	PRA*	RBU*	MGA	CRT
Add, search for, change and verify payer profile													X			
View payer profile reports													X			

7.6 Transactions Search (Agency Collections / My Agency Website)

Permissions Transaction Search	Public	PGE	AFL*	AFF*	ROA*	ACS*	BIG*	BAG*	CPA*	COS*	COE*	PPA*	PRA*	RBU*	MGA	CRT
Search for and view transactions						X				X	X					
Submit Plastic Card Force										X						
Issue Plastic Card Refund											X					
Void Plastic Card Transaction											X					
Cancel Plastic Card Transaction																
Cancel Deferred Plastic Card Transaction																

Permissions Transaction Search	Public	PGE	AFL*	AFF*	ROA*	ACS*	BIG*	BAG*	CPA*	COS*	COE*	PPA*	PRA*	RBU*	MGA	CRT
Cancel Recurring Plastic Card Transactions																
Cancel ACH Debit											X					
Cancel Deferred ACH Debit											X					
Cancel Recurring ACH Debit											X					
Edit ACH Debit											X					

7.7 Reports (Agency Collections / myagency Website)

Permissions Reports	Public	PGE	AFL*	AFF*	ROA*	ACS*	BIG*	BAG*	CPA*	COS*	COE*	PPA*	PRA*	RBU*	MGA	CRT
Access Agency Collections (myagency) website					X		X	X		X	X					
Activity File Download					X	X				X	X					
Adapter File Status					X	X				X	X					
Billing Search					X	X				X	X					
Collection Voucher Report					X	X				X	X					
Collection Search CSV Download					X	X				X	X					
Company Profile User Report									X							
Company Profile Values									X							
Email Exceptions					x	x				x	x					
Financial Summary Report					X	X				X	X					
Form Search					X	X				X	X					
Notification of Change Search					X	X				X	X		X			
Payer Profile Audit Log													X			
User Access Report						X										
View transaction details (ACH)										X	X		X			
View transaction details (plastic card, ecomm)					X	X				X	X					
Transaction Search					X	X				X	X		X			

7.8 Activity Files

Permissions Download Activity Files	Public	PGE	AFL*	AFF*	ROA*	ACS*	BIG*	BAG*	CPA*	COS*	COE*	PPA*	PRA*	RBU*	MGA	CRT
ACH Activity File															X	
Adapter Activity															X	
Billing Activity File															X	
CBP Duties Activity File															X	
CC Activity File (Credit Card)															X	
Collections Activity File															X	
Collections Activity File v2															X	
Collections Activity File v3 (XML or JSON)															X	
Collections Activity File v4 (XML or JSON)															X	
Digital Wallet Activity File															X	
Form Activity File															X	
Form Activity File v2 (XMl or JSON)															X	
Form Activity File XSL															X	
Form Attachment Activity Files															X	

> ***Note:*** A separate account with the MGA role is required to download Activity Files using the Activity File Service or Activity File Servlet. A machine account (MGA role) is required for system-to-system downloads.

7.9 TCS Web Services, Hosted Collection Pages

Permissions TCS Web Services, eBilling Service, Hosted Collection Pages	Public	PGE	AFL*	AFF*	ROA*	ACS*	BIG*	BAG*	CPA*	COS*	COE*	PPA*	PRA*	RBU*	MGA	CRT
Access TCS, and Hosted Collection Pages Web Services																X

7.10 TCS Certificate Account

Permissions Access to Web Service	SRC	SQC	MQC*	BTC*	BRC*	BIL	ACC*
TCS Single Service	X						
TCS Single Query Service		X					
Multiple Item Query Service			X				
TCS Batch Service				X			
TCS Batch Results Service					X		
eBilling Web Services						X	X
eBilling Online Web Service						X	X

Important! Both the BIL and ACC roles are required for certificates accessing the eBilling Web Services or the eBilling Online Web Service.

7.11 Agency User Recertification

Permissions User Recertification	Public	PGE	AFL*	AFF*	ROA*	ACS*	BIG*	BAG*	CPA*	COS*	COE*	PPA*	PRA*	RBU*	MGA	CRT	SEC
Review agency user roles and application access																	X
Request adding agency users																	X
Request deleting agency users																	X
Request adding roles or application access for an agency user																	X
Request deleting roles or application access for an agency user																	X

8 Requirements

8.1 Security Contacts

Only your agency's authorized Pay.gov Security Contacts can request access and assign user roles for your collection applications.

Your agency must have at least two individuals as your authorized Pay.gov Security Contacts; you may designate more.

- Your initial security contacts must be designated at the time your agency is set up on Pay.gov.
- Include Security contact information in the Agency Configuration Template (ACT), which is available at https://qa.pay.gov/agencydocs/docs/act_blank.doc.
- In the ACT, you may select specific collection applications that the security contacts are responsible for, or you may have the security contacts responsible for all your applications.

Designated security contacts agree to abide by the terms and conditions listed in the Notices and Agreements document posted at https:pay.gov/myagency/#/information-and-resources#rob.

8.1.1 Security Contact Responsibilities

- Requesting access in Pay.gov's agency testing and production environments and for the public website and/or the agency website.
- Requesting and modifying user access and roles (agency user and agency-registered PGE) for the applications they are responsible for.
- Requesting credentials for Collections API.
- Ensuring that Collections API credentials are updated before they expire.
- Removing user access to applications.
- Requesting new or replacement Security Contacts.
- Removing Security Contacts.
- Ensuring that the machine account ID password is changed:
  - At least annually (machine account passwords do not automatically expire.
  - When a user no longer has a need to know the password because of a change in job duties, termination of employment, etc.
  -

> ***Important!*** Security contacts may not request additions or changes to their own access permissions. Request must be submitted by another authorized security contact for their agency's applications. See section 8.2

8.1.2 Adding and Replacing and Deleting Additional Security Contacts

Once established, the initial security contacts may submit a *Designation of Security Contacts* form to

- designate additional security contacts
- replace previously designated security contacts
- remove existing security contacts

Changes must be approved by a current security contact for that agency or by the Bureau of the Fiscal Service. Your agency must always have two security contacts.

The Designation of Security Contacts form is available at https://qa.pay.gov/agencydocs/docs/designation_of_security_contacts_form.pdf

8.2 Rules for Access Requests

Access request rules ensure the integrity, confidentiality, and availability of the Pay.gov system. These rules are as follows:

- Requests are only accepted from an authorized agency security contact.
- Requests can only be made by submitting the appropriate Access Request Worksheet (ARW) to Pay.gov (pay.gov.application.requests@clev.frb.org).
- An agency security contact may request access for others, but they may not request their own access without authorization by another security contact. The secondary security contact's name and contact information must be listed on the required information worksheet. The secondary security contact must also be copied on the email when the access request is sent to the Pay.gov Application Security department at the Federal Reserve Bank of Cleveland (FRB-C). Any exceptions to this rule must be approved by the Pay.gov Information Systems Security Officer.
- Security contacts may not request access to reports, forms, or bills that belong to other agencies.
- Access requests must include the required information worksheet as well as the appropriate worksheet for the type of access desired.
- Requests for accounts to be used for uploading billing files and/or downloading reports without manual intervention (machine accounts to be used for the download of activity files), must only be used for that purpose, and will be assigned the ROA role exclusively.
- Whenever possible, requests should be submitted at least four business days in advance of when the access is required.

9 Procedures

The following sections provide the steps and responsible parties for the initial security contact assignment and the access request process. Please refer to the *Agency Guide to Company Profiles* for procedures related to company profile administration.

9.1 Security Contact Assignment, Change, or Removal

Step	Description	Responsible Party
1.	Designate initial security contacts when completing your agency's ACT. They are established during the ACT approval process. After this approval process is completed, users can request access to the test system. Note that a final move-to-production signoff for the completed ACT, initiated by the Pay.gov program manager or designee, must be sent to Pay.gov before a production access request will be completed.	Agency and the Bureau of the Fiscal Service
2.	Updates to existing, approved agency security contacts may be completed using the Pay.gov Designation of Security Contacts form.	Agency security contact

9.2 Access Requests

You must submit the appropriate ARW for the Pay.gov service your application users to create and modify users and their roles. See section 2.5 for ARW descriptions.

9.2.1 Create New Users

Step	Description	Responsible Party
1.	Open the appropriate Pay.gov ARW in Excel.	Security Contact
2.	Complete the "Required Information" worksheet (the information required is the same for all spreadsheets).	Security Contact
3.	Complete the "Create New User" worksheet with the required information for the users to be created.	Security Contact

Step	Description	Responsible Party
4.	Complete the "Assign User Roles" worksheet to request roles for the new users. Available roles vary according to the ARW used. Form access is granted at the application level. Users assigned a form access role will have access to all forms for the application(s). See sections 9.4 if scope access is required and section 9.5 if filling out a spreadsheet for forms and company profile information.	Security Contact
5.	Save and close the Excel file.	Security Contact
6.	Email the Excel file to pay.gov.application.requests@clev.frb.org.	Security Contact
7.	Pay.gov verifies that the request was sent by one of the agency's security contacts and that the form has been properly completed. The submitting security contact will be informed if the ARW has been rejected, including the reason for rejection.	Pay.gov Application Security
8.	Pay.gov creates the usernames. The system will automatically generate the usernames and will email them to the users.	Pay.gov Application Security
9.	Pay.gov assigns the appropriate roles to the users.	Pay.gov Application Security
10.	Provide a temporary password to the users.	Pay.gov Application Security *or* Security Contact
11.	Pay.gov notifies the security contact that the request has been completed.	Pay.gov Application Security

9.3 Modify User Roles

Step	Description	Responsible Party
1.	Open the appropriate Pay.gov ARW in Excel.	Security Contact
2.	Complete the "Required Information" worksheet.	Security Contact
3.	Skip the "Create New User" worksheet.	Security Contact

Step	Description	Responsible Party
4.	Complete the "Assign - Remove User Roles" worksheet. Enter the users first and last name. Select the application they have access to from the dropdown list. Enter A in the column for the role being added, or R in the column for the role being removed. The roles available vary according to the ARW. Form access is granted at the application level. Users assigned a form access role will have access to all forms for the application(s). *or* Complete the "Delete existing users" worksheets to remove the user account(s) from the Pay.gov system. See sections 9.4 if filling out a spreadsheet for modifying form scope and section 9.5 if filling out a spreadsheet to modify company profile information.	Security Contact
5.	Save and close the Excel file.	Security Contact
6.	Email the Excel file to pay.gov.application.requests@clev.frb.org	Security Contact
7.	Pay.gov verifies that the request was sent by one of the agency's security contacts and that the form has been properly completed. The submitting security contact will be informed if the ARW has been rejected, including the reason for rejection.	Pay.gov Application Security
8.	Pay.gov assigns or removes the roles. *or* Delete the user(s).	Pay.gov Application Security
9.	Pay.gov notifies the security contact that the request has been completed.	Pay.gov Application Security

9.4 Adding/Update Scope Information

Scope is not available for new applications. Support is maintained for existing applications already using scope information. Agencies needing to modify scope

information for an application should contact their Pay.gov Agency Implementation Liaison.

9.5 Add/Remove Company Profile Information

Step	Description	Responsible Party
1.	List the first name and last name for each user to be added to one or more company profiles.	Security Contact
2.	List the company profile IDs and company profile names for each user and indicate whether they are to be added to or removed from the user account.	Security Contact

9.6 Request Collections API Credentials

Step	*Description*	*Responsible Party*
1.	Submit the Authorization User Account Access Request Worksheet.	Security Contact
2.	Pay.gov creates the API role for the cash flow application,	Pay.gov
3.	Pay.gov creates the Collections API credentials and agency signature.	Pay.gov
4.	The agency is notified by email when credentials are available.	Pay.gov
5.	Notify Pay.gov of the date and six-hour time range when you will be able to download the credentials.	Security Contact
6,	Receive an email providing the one-time URL for the download.	Pay.gov
7.	Download the credentials. Note that the download is available for six hours only, after which it is no longer available and must be requested again.	Security Contact

10 Support

10.1 Customer Support

Hours:8:00 am to 7:00 pm Eastern Time

Monday through Friday, Closed Bank Holidays

Phone:(800) 624-1373

Email address:pay.gov.clev@clev.frb.org

10.2 Pay.gov Application Security

The Pay.gov Application Security team may be contacted by email at pay.gov.application.requests@clev.frb.org.