Central Governance

Version 5.0

7 July 2021

Access and Security

This documentation describes the following Axway software:

Axway Central Governance - Access and Security

Contents

Getting started with Central Governance Access and Security 1

The following topics introduce concepts for using Access and Security.

Using the UI and help

The following topics provide information about using the user interface and online help.

Supported browsers

The supported browsers for this UI are the same as for Central Governance. Please see the Central Governance Users Guide.

Monitor resolution

The suggested minimum monitor resolution setting for using this UI is 1024 by 768. Even set at this minimum, you may have to use the UI in maximized mode. If you experience issues in maximized mode at the suggested minimum resolution, increase the resolution settings.

Time outs

If you have logged on but are inactive for a while, the browser session times out, forcing you to log on again. The length of the idle period preceding time outs is set by the administrator.

Using help

You can open the Access and Security help documentation by clicking **Help** on the top toolbar in the user interface. You can open context-sensitive help by selecting **Help > Help Topic**.

If you experience any display or linking problems with the help, clear the browser's cache and try again.

Grid preferences

For pages that display lists of Access and Security objects (for example, users, groups, organizations), you can control the information displayed and its order. Click the **Grid Preferences** icon on the right side of a window to open the Grid Preferences dialog box. By default, all fields are displayed and listed in the right pane of the dialog box. Do the following to change the grid's appearance:

- Drag field names up and down in the right pane to change their order.
- Drag fields from the right pane to the left to remove them from view.
- Drag fields from the left pane to the right to display them.
- Select one or more fields in either pane and click the right or left arrow to move to the other pane. Use the **Ctrl** key to select more than one field.

Searching lists of objects

For pages that display lists of Access and Security objects (for example, users, groups, organizations), you can search for a particular object. The search feature is the same from page to page, but the search criteria differ as appropriate for the objects in question.

To show the search fields, click **Search** or the arrow at the top left of a window to expand the search fields. By default, the search fields are collapsed.

To search for an object in a list, enter some search criteria and click **Go**.

PassPort menus in Central Governance

Central Governance relies on an embedded PassPort for some screens and functionality. In some instances, there may be a discrepancy between the screens described in the PassPort documentation and the screens available in a Central Governance implementation.

Axway Desktop Client

As of January 12, 2021, Adobe blocked Flash content from running in Flash Player, which Central Governance used to access the **Access and Security** features. To enable the use of Access and Security in the same graphical user interface as before, you can download Axway Desktop Client from the Axway support site.

Access and Security UI Lite

Axway provides a new user interface as of 2021, **Access and Security UI Lite**, to enable the use of Access and Security services.

- If you are using Central Governance SP16 and lower, download Access and Security UI Lite from the Axway support site.
- If you are using Central Governance SP17 and higher, Access and Security Ui Lite is integrated in the Central Governance delivery.

Note This *User Guide* describes the old user interface, which differs somewhat from Access and Security UI Lite. Refer to *Access and Security UI Lite* information available in the Central Governance 1.1.3 SP17 Readme for supported features and limitations.

Getting started with Security service

Security service offers security by providing authentication, confidentiality, integrity and non-repudiation of documents. Security service uses state-of-the-art cryptography to ensure the security of the documents exchanged over the public Internet.

Security service supports public key infrastructure (PKI). PKI is a system of components that use digital certificates and public key cryptography to secure transactions and communications.

Security service supplies security services, including:

- Authentication, confidentiality, integrity and non-repudiation of data
- Advanced functions such as time stamps and automated certificate and key processes

It also delivers management services, including:

- Creating, publishing and revoking certificates
- Storing certificates and keys
- Managing the lifecycle of keys (renew, archive, recover)

For information about using Security service, see *Managing certificates and keys* on page 22.

Certificate basics

The following topics describe the use of digital certificates in Security service.

PKI description

Access and Security supports public key infrastructure (PKI). **PKI**[1]s a system of components that use digital X.509 certificates and public key cryptography to secure transactions and communications.

PKI uses certificates issued by certificate authorities (CAs) to provide authentication, confidentiality, integrity and non-repudiation of data. The following defines these in more detail.

[1]Public key infrastructure is a set of hardware, software, people, policies and procedures for creating, managing, distributing, using, storing, and revoking digital certificates.

Authentication

Authentication is verification of the identity of a person or process. Authentication confirms that a message truly came from the source that sent it.

Confidentiality

Confidentiality is the assurance that a message has been disclosed only to the parties authorized to share the information.

Integrity

Integrity is the assurance that the information has not been altered in any way and is precisely true to the source.

Non-repudiation

Non-repudiation is proof that a recipient received a message. This protects a sender from a false denial that a recipient did not receive a message.

Entity association

Every certificate in Access and Security must be associated with exactly one certificate entity.

If multiple end-entity certificates issued by the same certificate authority are to be used within Access and Security, the CA root and intermediary certificates must be in different entities from the end-entity certificates. Access and Security has default entities to store intermediate and root CA certificates.

An administrator with security privileges must create entities to store end-entity certificates of local organizations. However, Access and Security manages entities of remote organizations without user intervention.

About the default entities

Security service has the following default entities for certificates:

- Intermediate CA Certificates is provided as a container of intermediate certificates issued by CAs. The entity password is **intermediate**.
- Root CA Certificates is provided as a container of root certificates issued by CAs. The entity password is **root**.
- SSL is provided as a container of SSL certificates. The entity password is **ssl**.

Because passwords of the default entities are known, do not add private keys to them.

Intermediate and root certificate entities

The Intermediate CA Certificates and Root CA Certificates entities must contain the intermediate and root certificates related to the end-entity certificates used by the server or local and remote organizations. Security service must reference intermediate and root certificates when building and validating chains of trust. The server does this by building the trust path from the end-entity certificate to its root certificate. All certificates within the chain must be activated and at least one certificate in the path must be trusted.

The server adds certificates to the entities as part of the normal process of adding end-entity certificates for the server or local and remote organizations. For example, a user wants to import to a local organization's entity an end-entity certificate, which could be a P12 file containing a public-private key pair of a local organization or a P7 file containing only a public key of a remote organization. But the certificate also contains a chain of intermediate and root certificates. Security service imports the end-entity certificate to the local organization's entity, but adds the intermediate and root certificates within it to the Intermediate CA Certificates and Root CA Certificates entities.

An administrator with security privileges can trust or un-trust the Intermediate CA Certificates and Root CA Certificates entities. An administrator also can open the entities and view certificates and details about them.

Do not import certificates to these default entities, as the role of the entities is only to store intermediate and root certificates in certificate chains. To store user certificates, add a dedicated entity with a secured password.

An administrator can delete the default entities and all certificates within them, but that is strongly discouraged. Although the server creates the entities again when restarted; any deleted certificates are not restored.

You must use the default entities as stores of intermediate and root certificates. Do not add an entity of your own to use for this purpose.

When adding or editing a local organization, do not associate a organization with one of the default entities. A local organization must be associated with an entity added specifically for use by the organization to store its end-entity certificates and keys.

About self-signed certificates

The self-signed certificates you can generate in Security service are both end-entity and root certificates. You are, in effect, your own CA when you generate a self-signed certificate. The server does not add to the Root CA Certificates entity any self-signed certificates you generate or import to a local organization entity.

Importing certificates

Access and Security can import PKCS#7 (typically .p7b or .p7c) files that contain more than one certificate (for example, a certificate chain). When a certificate chain is encountered, intermediate certificates within the chain are imported to the default Intermediate CA Certificates entity and root

certificates are imported to the default Root CA Certificates entity.

When importing a .p12 or .pfx file that contains a private key, Access and Security imports the private key and the certificate associated with the key. Access and Security also can import the certificate chain, adding intermediate and root certificates to the appropriate default entities.

Access and Security expects imported .cer files to contain the raw binary of the DER encoding of a certificate, while it expects .crt files to contain the base-64 encoding of a DER-encoded certificate. Access and Security can determine the format of the data inside these files, but enforces that the data format match these extension rules.

See *Importing PGP keyrings for ElGamal* on page 25 for details about importing PGP keyrings.

External resource

See RFC 3280 (http://www.ietf.org/rfc/rfc3280.txt) for complete information about Internet X.509 public key infrastructure.

Axway support

Go to Axway Sphere at support.axway.com to contact a support representative, learn about training programs, or download software, documentation and knowledge-base articles. The website is for customers with active Axway support contracts. You need a user name and password to log on. Post comments and question to the Axway user forum at forums.axway.com/index.php.

Access menu 2

This section provides topics about using the Access menu for Access service.

Roles and privileges

Privileges are the permissions to perform specific actions, either in Access and Security or another Axway product. Each privilege is associated with a specific product. Roles are a collection of privileges. You can assign roles to users, organizations or user groups..

The user interface subdivides privileges as user-defined and predefined. There are some usability differences between the two. User-defined privileges can be associated with conditions of use. Predefined privileges exist by default or have been imported from a **component security descriptor file**[1]. You can delete user-defined privileges, but not predefined privileges. You can copy a predefined privilege and paste it in the Privileges page to use as a template for a new user-defined privilege.

Likewise, the UI subdivides roles as user-defined and predefined. Predefined roles exist by default or have been imported from CSD files. You can assign roles to users, organizations and groups. You can copy a predefined role and paste it in the Roles page to use as a template for a new user-defined role. When you copy a role, its privileges but not its users are copied. Roles are also hierarchical, allowing for aggregate groupings of privileges associated with those roles.

User privileges

The following topics describe user privilege tasks you can perform on the Access menu.

Add a privilege from a resource

Use this procedure to add a user privilege from a resource. Privileges are based on resources, and a single privilege is based on a single resource. Most resources come from component security descriptor files, but a pool of resources exist by default for Access and Security. To add a privilege for a **product**[2] other than Access and Security, the product's CSD file must be imported first.

If a CSD file contains predefined privileges, you may not need to add privileges manually. The file may provide a group of privileges that meet your needs.

[1]Component security descriptor (CSD) files are XML files that define product resources, user privileges and user roles for each product that integrates with AM for identity and access management.
[2]Axway business application software. Also known technically in PassPort as a component.

This procedure is one of two ways to add a privilege. The other is *Add a privilege by copying* on page 12.

1. Select **Access > Privileges**.
2. Click **New Privilege**.

General information

3. Type a name and optionally a description. Accept the default status (active) and default selection of the Static check box. Click **Next**.

Select product, resource, actions

4. Click the magnifying glass icon next to the Resource field.
5. Select from the drop-down list the product on which to base the privilege.
6. Select from the list the resource to associate with the privilege and click **OK**.
7. Select at least one action for the resource. If there are multiple actions and you are unsure which to select, select all.
8. Click **Finish** to add the privilege.

   The **Next** option opens a page for associating one or more conditions to the privilege. That optional process is described in *Use the privilege condition editor* on page 16.

After adding a privilege you can:

- View or change details about it.
- Change its status.
- Delete it.
- Add it to a role.

Add a privilege by copying

Use this procedure to add a privilege by copying an existing privilege.

This is one of two ways to add a privilege. The other is *Add a privilege from a resource* on page 11.

1. Select **Access > Privileges**.
2. Find the predefined privilege you want to copy. You cannot copy a user-defined privilege.
3. Select the privilege and click **Copy** and then **Paste**.
4. When prompted, type a unique name for the privilege and click **OK**.
5. To change any attributes or actions, click the privilege name. to edit and click **Save** when done.

   For information about privilege conditions see *Use the privilege condition editor* on page 16.

After adding a privilege you can:

- View or change details about it.
- Change its status.
- Delete it.
- Add it to a role.

About the privilege condition editor

When adding or editing a user-defined privilege, use the condition editor to add or change conditions for using the privilege. You cannot edit conditions of predefined privileges.

You can base conditions on user-defined or default properties. User-defined properties are specified when adding or changing groups or users. Product resources also may have properties.

The following topics provide a condition example and describe group, user and system properties and also operators for properties.

Condition example

Conditions can be used to specify when a user or group can use privileges. Conditions can be associated with groups and linked to privileges as a way to trigger when users in the group can use privileges.

For example, if you add a property-value pair of **Property A = 1** to a group, you can set the same pair for a privilege. This has the effect of enabling users assigned to the group to use the privilege. However, if you set **Property A = 2** to the privilege, the group's users could not use the privilege.

Group properties

Group properties are user defined properties that are in use by one or more groups. These properties, if any, apply only to users in groups that use the properties.

User properties

User properties are user-defined properties that are in use by one or more users. These properties, if any, apply only to users that use the properties.

System properties

The system properties that can be applied to conditions are:

componentId

Links a privilege to an instance of a product. Component ID has the same meaning as an instance as used in **Access > Products**.

componentName

Links a privilege to a product.

componentGroup

Links a privilege to a product parent group. The only valid component group is Synchrony.

componentOrganizationName

Links a privilege to an organization name or partial name.

componentVersion

Links a privilege to a version of a product.

componentOrganizationName

Links a privilege to a component organization.

currentTime

Links a privilege to a time. The condition can specify whether a privilege is enabled before, after or during the set time.

currentDate

Links a privilege to a date. The condition can specify whether a privilege is enabled before, after or during the set date.

currentDateTime

Links a privilege to a date and time. The condition can specify whether a privilege is enabled before, after or during the set date and time.

currentWeekDay

Links a privilege to a day of the week. The condition can specify whether a privilege is enabled before, after or during the set day.

currentYear

Links a privilege to a year. The condition can specify whether a privilege is enabled before, after or during the set year.

currentMonth

Links a privilege to a month. The condition can specify whether a privilege is enabled before, after or during the set month.

currentDay

Links a privilege to a day of the month. The condition can specify whether a privilege is enabled before, after or during the set day.

IP

Links a privilege to the IP address of the computer running a product that is integrated with Access and Security.

localHostName

Links a privilege to the name of the computer running a product that is integrated with Access and Security.

UserDomain

Links a privilege to a domain.

UserID

Links a privilege to a user.

Operators for properties

All default properties, except those related to dates or times, have the following available operators.

Use of wildcard characters is allowed as noted. Valid wildcards are:

- ***** (asterisk) Any characters zero or more times
- **?** (question mark) Any single character

is

The privilege is enabled only when a matching value is the same as this value. Do not use wildcard characters with this operator. For example, if the property is componentId and the value is **default**, the privilege can be used with a product with an instance name of default.

starts with

The privilege is enabled when a matching value starts with this character or characters. Wildcards allowed. For example, if the property is componentId and the value is **d**, the privilege can be used with a product with an instance name beginning with that letter.

ends with

The privilege is enabled when a matching value ends with this character or characters. Wildcards allowed. For example, if the property is componentId and the value is **t**, the privilege can be used with a product with an instance name ending with that letter.

contains

The privilege is enabled with a matching value includes the specified character or characters. Wildcards allowed. For example, if the property is componentId and the value is **fa**, the privilege can be used with a product with an instance name including those letters.

like

Use wildcards with this operator to perform pattern matching.

Negation

Negation (not) can be specified for **and-or** conditions and any property. The **!** character represents negation. Negation is an operation on a logical value that produces a value of true when its operand is false and a value of false when its operand is true. For example, if **A** is true then **not A** is false. Conversely, if **not A** is true then **A** is false.

Use the privilege condition editor

Use this procedure to add or change conditions for new or existing privileges.

For more information see *About the privilege condition editor* on page 13.

1. Select **Access > Privileges**.
2. Add a privilege or open an existing user-defined privilege.
    - To add, click **New Privilege** and click **Next** until you reach Edit Conditions.
    - To open, click a privilege name and click the **Condition Editor** tab.
3. Set up a single condition or multi-part condition. For a multi-part condition, you can set up **and-or** operators You also can specify negation.

    For a single condition, double-click **undefined** and select a property, operator and value.

    For a multi-part condition, click **Condition** and double-click **undefined** to add a property and value. Or, click **Operator** to add another **and-or** condition (double-click **AND** or **OR** to toggle between the two). Type or select a value.

    Click **From a PassPort object** to base a condition on a user or contact or a product. If you select a user or contact, the editor sets the user ID and domain for the user or contact. If you select a product, the editor sets the product instance, group and name. You can select only one object.

    If the property you want is not available, go to **Access > User Groups** and add a property-value pair to a group or **Community > Users and Contacts** and add a property-value pair to a user.
4. Click **Finish** or **Save** to save your changes.

User roles

The following topics describe user role tasks you can perform on the Access menu.

Add a role based on privileges

Use this procedure to add a role based on one or more privileges.

This is one of two ways to add a role. The other is *Add a role by copying* on page 18.

1. Select **Access > Roles**.
2. Click **New Role**.

General information

3. Type a name and optionally a description. Accept the default status of active or change it to inactive, which makes the role unavailable.

   Click **Next** to add privileges. Or, click **Finish** to add the role without adding privileges to it. You can add privileges later. You also can click **Finish** at any later point in the wizard to skip next steps.

Select privileges

4. Add one or more privileges to the role. Do one of the following. When performing a search you can use the wildcards * and ? to substitute for characters.
   - If you know the full or partial name of the privilege, type it and click **Search** to list the privilege.
   - Type the full or partial name of the **product**[1] and click **Search** to list associated privileges.
   - Type the full or partial name of a resource and click **Search** to list any privilege associated with the resource.

   Use the arrows to add or remove privileges.

   When a search returns a list of privileges, place the cursor over names to display descriptions of the privileges. Descriptions display only for Access and Security privileges, products whose imported CSD files contain privilege descriptions and user-defined privileges with descriptions.
5. Click **Next** to add users.

Select users

6. Optionally, search for users and add one or more to the role. Type the full or partial name of a user and click **Search** or click **Search** without typing to find all users. Use the arrows to add or remove users.
7. Click **Next** to add groups.

Select groups

8. Optionally, search for groups and add one or more to the role. Type the full or partial name of a group and click **Search** or click **Search** without typing to find all groups. Use the arrows to add

[1]Axway business application software. Also known technically in PassPort as a component.

or remove groups.

9. Click **Next** to add sub-roles.

Select sub-roles

10. Optionally, search for roles and add one or more as sub-roles. Type the full or partial name of a role or a product and click **Search** or click **Search** without typing to find all roles. Use the arrows to add or remove sub-roles.
11. Click **Finish** to add the role.

After adding a role you can:

- View or change details about it.
- Change its status (active or inactive)
- Delete it after deactivating.

Add a role by copying

Use this procedure to add a role by copying an existing role. Role copying duplicates the privileges in the original, but not other attributes (such as associated users).

This is one of two ways to add a role. The other is *Add a role based on privileges* on page 16.

1. Select **Access > Roles**.
2. Find the predefined role you want to copy. You cannot copy a user-defined role.
3. Select the role, click **Copy** and then **Paste**.
4. Type a unique name for the copied role and click **OK** to add it. The copied role displays as a user-defined role.

After adding a role you can:

- View or change details about it.
- Change its status (active or inactive)
- Delete it after deactivating.

About role types

There are differences between managing user-defined and predefined roles.

User-defined roles

You can add or remove privileges and other attributes. As these roles are user-defined, all changes are allowed. However, you cannot copy user-defined roles.

Predefined roles

You can add or remove users, organizations, groups and sub-roles. However, you cannot change privileges within predefined roles, as this would change the nature of the roles. You can deactivate but not delete predefined roles. Predefined roles are either default roles or imported from CSD files.

You can set up relationships among roles in a parent-child hierarchy. Under this concept, one role can serve as an container of many related or unrelated sub-roles.

When adding users to a role, you can add users individually or add an organization or group, which adds all of its users to the role at once.

Manage roles

Use this procedure to mange roles. This includes adding or removing users, privileges and sub-roles.

1. Select **Access > Roles**.
2. Click the name of a role to view or change its properties.
3. Click the tab you want and use the arrows to add or remove properties. Click **Save** to retain any changes.

Conditional user roles

Access and Security supports **products**[1] that register, via the API, instance groups supporting conditional roles for users. Conditional roles are the same as normal roles, except users can exercise the roles only under certain conditions.

The following topics provide more information about conditional roles.

Why use conditional roles

A product may have dozens or hundreds of individual installed instances registered in Access and Security. The instances may represent different versions of the product, or the instances may be geographically diverse. An administrator may want privileges of some users restricted to certain product versions or limited to product instances in a specific region. Administrators of products that register instance groups with Access and Security can set such boundaries.

Enabling conditional roles

Use of conditional roles is enabled and disabled by setting a property under Administration > System Properties. The property is:

[1]Axway business application software. Also known technically in PassPort as components.

`am.enable.conditional.roles`

The property default value is **false**, which disables conditional roles. Set the value to **true** to enable.

Enabling the property activates user interface pages related to conditional roles under:

- Administration > Products
- Community > Users and Contacts
- Access > User Groups

However, you can use this UI only when at least one product has registered instance groups for conditional roles via the Access and Security API. Instance groups are in addition to product roles provided by a component security descriptor file. The CSD file must be sent to Access and Security via the API when the product self registers or imported manually in the UI under Administration > Products.

Check a product for instance groups

Use this procedure to check whether a product instance has instance groups for conditional roles.

1. Select **Administration > Products** and click a product name to open the Product Details page.
2. Review the Instance Group column for whether the instance has an assigned instance group.
3. To change or assign an instance group:
    a. Click the name of a product instance.
    b. Click the magnifying glass icon next to the Instance Group field.
    c. Select an instance group and click **OK**.

Assign conditional roles to a user

Use this procedure to assign conditional roles to a user.

This procedure traces assigning conditional roles to a new user. For an existing user, select **Community > Users and Contacts**, click the name of a user and click the **Conditioned Roles** tab. Assigning conditional roles on this tab for an existing user is the same as when assigning for a new user in the following procedure. Click **Save** when done.

1. Select **Community > Users and Contacts** and click **New User/Contact**.
2. Enter information for the new user in the wizard. Click **Next** to select groups and roles, as needed.
3. When you reach the Select Conditioned Roles for User page, use the arrows to assign available roles as conditional roles. Selected roles display in the Selected Roles area of the page.
4. Select one of more of the selected roles and do the following:
    - Click **Set Products** and select one or more product instances. This means the role is active for the user only when the user activity affects the selected product instances. Click **OK**.

- Click **Set Instance Groups** and select one or more instance groups. This means the role is active for the user only when the user activity affects the product instances defined in the instance groups. Click **OK**.

5. Click **Finish** to add the user.

Assign conditional roles to a user group

Use this procedure to assign conditional roles to a user group. Users assigned to a user group inherent any conditional roles assigned to the group.

This procedure traces assigning conditional roles to a new user group. For an existing user group, select **Access > User Groups**, click the name of a user group and click the **Conditioned Roles** tab. Assigning conditional roles on this tab for an existing user group is the same as when assigning for a new user group in the following procedure. Click **Save** when done.

1. Select **Access > User Groups** and click **New User Group**.
2. Enter information for the new user group in the wizard. Click **Next** to select users and roles, as needed.
3. When you reach the Select Conditioned Roles page, use the arrows to assign available roles as conditional roles. Selected roles display in the Selected Roles area of the page.
4. Select one of more of the selected roles and do the following:
   - Click **Set Products** and select one or more product instances. This means the role is active for the user group only when the user activity affects the selected product instances. Click **OK**.
   - Click **Set Instance Groups** and select one or more instance groups. This means the role is active for the user group only when the user activity affects the product instances defined in the instance groups. Click **OK**.
5. Click **Finish** to add the user group.

Security menu 3

This section provides topics about using the Security menu.

Managing certificates and keys

The following topics describe managing certificates and keys using the Security menu.

Only authorized users can manage certificates and keys.

Note When using the *Access and Security Lite* user interface, some menus may differ from those described in this document.

For concepts about certificates,see *Certificate basics* on page 7 .

Add an entity

Use this procedure to add an entity as a container for certificates and keys. Before you can import or add certificates or keys for a local organization, you must create an entity. You also must add at least one entity before Access and Security allows you to add a local organization under the Community menu.

1. Select **Security > Entities** and click **New Entity** to open the Create Entity page.
2. Type a name, select a domain and, optionally, select the Trusted check box.

   Type a password for the entity. Remember the password as you need it later to perform actions, such as importing.
3. Click **OK** to add the entity.

After adding an entity you can:

- Trust or un-trust an entity.
- Click the entity name to open a page for managing its certificates and keys, such as importing and generating.
- Change the entity's password.
- Delete the entity.

Change an entity password

Use this procedure to change the password of an entity. You must know the current password to change it.

1. Select **Security > Entities**.
2. Select check box for an entity and click **Change Password**.
3. Type the current and new passwords.
4. Click **Save** to change the password.

Import a certificate or key

Use this procedure to import a certificate or public key. You must know the entity password to import to an entity. If importing a private key, you must know the key password.

Do not add certificates to the Intermediate CA Certificates, Root CA Certificates or SSL entities. See *About the default entities* on page 8 for how these entities are used.

For information about importing PGP keyrings, see *Importing PGP keyrings for ElGamal* on page 25.

1. Select **Security > Entities** and click the name of an entity to open its Entity page.
2. Click **Import** under the Certificates or Public Keys section of the page, depending on whether you are importing a certificate or key.

   You can import the following file types:

   - PKCS #7 (*.p7b, *.der, *.pem)
   - DER-encoded PKCS #12 (*.p12, *.phx)
   - PEM (*.crt)
   - Cert (*.cer)
   - PKCS #8 (*.pk8)
   - DER (*.der)
   - PEM (*.pem)
3. Complete the fields:
   - **Entity Password** – Type the password to authenticate permission to change the entity.
   - **Alias** – Type any value to identify the certificate or key in the Access and Security UI.
   - **Select File** – Use the browse tool to select the file to import.
   - **File Password** – Type the password to access the file if it is password protected.
   - **OCSP Server Blacklist** – This applies to certificates and not keys. If the certificate has an OCSP server defined (the address of a server is provided in the AuthorityInfoAccess field of the certificate) select an option for handling the server in the Access and Security blacklist:
     - **Don't blacklist** – The certificate is imported with no action on the blacklist.
     - **Blacklist** – If the certificate has an OCSP server, the server is added to the blacklist if it is not in already in it.

- **Blacklist if server is unavailable** – If the certificate has an OCSP server, Access and Security first checks if the server is already in the list. If yes, Access and Security just imports the certificate. If not, Access and Security attempts to contact the server with this certificate. Access and Security blacklists the server if the server does not respond.

4. Click **OK** to import the certificate or key.

After importing a certificate or key you can:

- Click the name of the certificate or key to view its details.
- Trust or un-trust it.
- Delete it.

Generate a certificate or key

Use this procedure to generate a certificate or public key.

Do not add certificates or keys to the Intermediate CA Certificates, Root CA Certificates or SSL entities. See *About the default entities* on page 8 for how these entities are used.

1. Select **Security > Entities** and click the name of an entity to open its Entity page.
2. Click **Generate** under Certificates or Public Keys, depending on whether you are generating a certificate or key.
3. Complete the fields. See *Certificate fields* on page 24 or *Public key fields* on page 25.
4. Click **OK** to generate the certificate or key.

After generating a certificate or key you can:

- Activate and trust a certificate.
- Activate a key.
- Delete a certificate or key.

Certificate fields

Entity password is the password given when the entity was added (see *Add an entity* on page 22), unless it was changed later (see *Change an entity password* on page 22).

Alias is the name you give to the certificate.

Validity period specifies the beginning and ending dates for the certificate. Dates display as mm/dd/yyyy.

Key information specifies the key length (encryption strength ranges from 512 to 4096) and the key algorithm (RSA or DSA).

Distinguished name is the list of standard attributes as defined in RFC 3280. You only must complete the required fields.

Usage describes the functions the certificate can perform. This does not mean it is being used for that purpose, only that it can be. The **Advanced usage** link is for specifying more granular usages. If you intend to specify advanced usages, do not select any of the common usage check boxes (signature, encryption and TLS).

Public key fields

Entity password is the password given when the entity was added (see *Add an entity* on page 22), unless it was changed later (see *Change an entity password* on page 22).

Alias is the name you give to the key.

Key options specifies the key length (encryption strength ranges from 512 to 4096) and the key algorithm (RSA or DSA).

Generate a certificate version

Use this procedure to generate a certificate version. Typically, a version is generated before a certificate expires so a replacement certificate is in place immediately.

1. Select **Security > Entities** and click the name of an entity to open its Entity page.
2. In the Certificates area, click **Show versions** to display existing versions of the certificate.
3. Click **Generate a Version** or **Import a Version**.
4. Complete the fields. See *Certificate fields* on page 24.

   You are not prompted to enter an alias. The server gives the version the same alias as the original certificate.
5. Click **OK** to generate or import the certificate version.

Importing PGP keyrings for ElGamal

The following topics are about importing PGP keyrings to enable ElGamal security.

About ElGamal

You can import **PGP**[1] keyrings containing one master key of type **DSA**[2] or **RSA**[3] and a set of sub-keys. The PGP keyrings must have at least one sub-key. The mandatory sub-key type must be RSA for an RSA master key, and **ElGamal**[4] for a DSA master key.

[1]Pretty Good Privacy (PGP) is a data encryption and decryption system that provides cryptographic privacy and authentication for data communication.
[2]The Digital Signature Algorithm (DSA) is a U.S. government standard, or FIPS, for digital signatures.
[3]RSA is an algorithm for public-key cryptography based on the presumed difficulty of factoring large integers. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described it in 1978.
[4]In cryptography, the ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography that is based on the Diffie–Hellman key exchange.

This functionality enables ElGamal private key storage for performing signing and decryption operations. Keyrings typically are in files with the following extensions: PKR, SKR, ASC and PGP.

When the master key contains the private key in the imported file (extension SKR or ASC), a self-signed certificate is generated by associating the Subject Distinguished Name specified in the import wizard and the master public key. Each sub-key of type ElGamal, containing the public and private part, is stored as a key linked to the master certificate generated previously. All the other keys that are not ElGamal are ignored.

When only the public part of the master key is available, a CA service with a signing certificate must be specified to sign the master public certificate. If a ElGamal private sub-key is not found in the imported file, the import results in a stand-alone certificate with no sub-keys.

External resource

See RFC 2440 at the following link for complete information about PGP keyrings and ElGamal formats:

http://www.ietf.org/rfc/rfc2440.txt

Import PGP keyring

Use this procedure to import a PGP keyring. You must know the password of the Access and Security entity to import a keyring. You also must know the password of the file to import if it contains a private key.

1. Select **Security > Entities** and click the name of an entity to open its Entity page. Do not use one of the Access and Security default entities (Intermediate CA Certificates, Root CA Certificates and SSL).
2. Click **PGP Import** at the top of the Certificates side of the Entity page to open the Import PGP Certificate wizard.
3. Do the following:
   - Type the entity password to authenticate permission to change the entity.
   - Type an alias for the keyring, which can be any identifier you want.
   - Click **Browse** and select a file to import. Click the drop-down menu next to the file name field to display the types of files you can import.
   - If the file to import contains a private key (for example, a file with an ASC or SKR extension), type the file password. Importing fails unless the password is provided.
   - If a public keyring is being imported (for example, a file with a PKR extension), select a CA service as the signing entity. The private key certificate of the CA service is used to sign the master certificate if the master key contains only the public key.

   Click **Next**.
4. Complete the Subject Distinguished Name information for the master certificate.
5. Click **Finish** to import the certificate and sub-keys.

After importing a certificate with ElGamal sub-keys you can:

- Click the name of the certificate or key to view its details.
- If ElGamal private keys were imported, click **Show Keys** to display sub-keys and:
    - View the ElGamal sub-keys
    - Click on a sub-key to view is details
    - Activate sub-keys
    - Delete sub-keys
- Trust or un-trust it.
- Delete it and its sub-keys.

Index