MyID PIV

Version 12.2

Entrust CA Gateway Integration Guide

Lutterworth Hall, St Mary's Road, Lutterworth, Leicestershire, LE17 4PS, UK
www.intercede.com | info@intercede.com | @intercedemyid | +44 (0)1455 558111

Document reference: INT2014-12.2.0-PIV

December 2021

Copyright

Conventions used in this document

- Lists:
  - Numbered lists are used to show the steps involved in completing a task when the order is important.
  - Bulleted lists are used when the order is unimportant or to show alternatives.
- **Bold** is used for menu items and for labels.

  For example:
  - Record a valid email address in **'From' email address**.
  - Select **Save** from the **File** menu.
- *Italic* is used for emphasis:

  For example:
  - Copy the file *before* starting the installation.
  - Do *not* remove the files before you have backed them up.
- ***Bold and italic*** hyperlinks are used to identify the titles of other documents.

  For example: "See the ***Release Notes*** for further information."

  Unless otherwise explicitly stated, all referenced documentation is available on the product installation media.
- A `fixed width` font is used where the identification of spaces is important, including filenames, example SQL queries and any entries made directly into configuration files or the database.
- **Notes** are used to provide further information, including any prerequisites or configuration additional to the standard specifications.

  For example:

  Note: This issue only occurs if updating from a previous version.
- Warnings are used to indicate where failure to follow a particular instruction may result in either loss of data or the need to manually configure elements of the system.

  For example:

  Warning: You must take a backup of your database before making any changes to it.

Contents

1 Introduction

This document provides a step-by-step guide to the installation and configuration requirements to integrate the Entrust CA Gateway with MyID®.

See:

- section *1.1*, *Prerequisites*.
- section *2*, *Configuration*.
- section *3*, *Logging*.

1.1 Prerequisites

You must have an Entrust CA Gateway configured for redirecting API calls between the client and the Entrust CA.

Refer to your Entrust CA Gateway documentation for recommendations of the hardware and software requirements and how to configure the gateway.

1.1.1 Supported Entrust CA Gateway versions

MyID has been tested with the following:

- API version: 1.6
- Application version: 2.4.0

You can use Entrust certificates in the same way as any other certificates within MyID. You can issue certificates to cards or as soft certificates by specifying them in a credential profile.

1.1.2 Certificate revocation list

The MyID application server must be able to communicate with the Certificate Revocation List (CRL) location. The CRL is checked for validity whenever MyID connects to the CA.

2 Configuration

This section contains information on configuring the Entrust CA and MyID to integrate with each other, including:

- Archiving keys.

  See section *2.1*, *Key archival and recovery*.
- Client authentication.

  See section *2.2*, *Setting up client authentication for Entrust CA Gateway access*.
- Configuring the CA within MyID.

  See section *2.3*, *Set up the MyID Entrust certificate authority*.
- Extended attributes.

  See section *2.4*, *Adding policy extended attributes*.
- Certificate policies.

  See section *2.5*, *Enabling certificate policies*.
- Updating the CA.

  See section *2.6*, *Updating CA details*.
- Attribute mapping.

  See section *2.7*, *Attribute mapping for PIV systems*.
- Limitations.

  See section *2.8*, *Limitations*.

2.1 Key archival and recovery

MyID can archive keys on the Entrust server or locally within MyID.

The available **Archive Keys** settings are:

- **None** – the key is generated on the device.
- **Internal** – the key is archived in MyID.
- **EntrustRest** – the key is archived in the Entrust server.

If the `key_client_generated` certificate profile property is set to false, the **Archive Keys** option is set to **EntrustRest**; you cannot change this. Otherwise, the **Archive Keys** option is set to **None** by default; in this case, you can change the setting to **Internal** if required.

2.2 Setting up client authentication for Entrust CA Gateway access

Before you configure MyID for Entrust CA access through the Entrust CA Gateway, you must have a client authentication certificate to allow secure communication between MyID and the Entrust CA Gateway endpoint. Where multiple CAs are being managed through multiple endpoints, you may have to provide a client authentication certificate for each endpoint.

1. The client authentication certificate can be issued from any certificate authority if it is available to CAPI or CNG.

   Note: Do not enable strong private key protection on the certificate, as this may prevent processing of the request by the MyID account.

2. Once you have the client authentication certificate:

   a. Log on as the MyID COM+ user account that is used to run the MyID components.

   b. Install and save the certificate as a `.cer` file (in binary or Base64-encoded X.509 format).

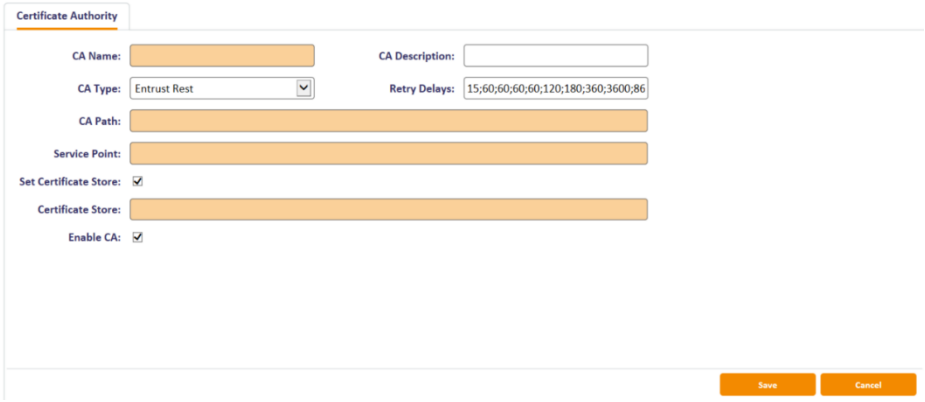
   c. Save the file in a location that is accessible to the MyID application on the application server.

2.3 Set up the MyID Entrust certificate authority

Note: MyID supports multiple Entrust CAs when accessed through Entrust CA Gateway endpoints.

To edit a Certificate Authority (CA):

1. From the **Configuration** category, select **Certificate Authorities**.
2. Click **New**.
3. From the **CA Type** drop-down list, select **Entrust Rest**.
4. Click the **Set Certificate Store** option.



5. Set the following fields:
   - **CA Name** – Enter the name that you will use to identify the CA.
   - **CA Description** – Enter a description for the CA.
   - **Retry Delays** – A semi-colon separated list of elapsed times, in seconds.

     For example, `5;10;20` means:
     - If the first attempt to retrieve details from the CA fails, a second attempt will be made after a `5` second delay.
     - If this second attempt fails, the CA will be contacted again after `10` seconds.
     - Subsequent attempts will be made to retrieve information every `20` seconds, until a response is received.

     If you want to limit the number of retry attempts, enter `0` as the last number in the sequence.
   - **CA Path** – Enter the identity assigned to the CA. Request this information through the CA administrator.
   - **Service Point** – This is the URL of the Entrust CA Gateway-hosted Rest API service.
   - **Certificate Store** – location of the client authentication certificate `.cer` file, as configured in section *2.2*, *Setting up client authentication for Entrust CA Gateway access*. For example:

     `C:\Certs\EntrustCert.cer`
   - Select **Enable CA** to make the policies available for issue.
6. Click **Save** to save these setting to the database. MyID is now ready to issue certificates.

2.4 Adding policy extended attributes

Entrust CA policies only specify mandatory extended attributes. The following XML configuration file:

`C:\Program Files\Intercede\MyID\Components\EntrustRestConnector.xml`

is used to add attributes to each of the Entrust CA policies. All custom extensions are defined in this file within an XML `<Extensions>` node. Each policy attribute is defined in an `<Extension>` node. Each attribute in the file specifies the following:

- `Name` – the type of extension. This may be:
  - `san` – A Subject Alternative Name.
  - `dn` – A subject DN component.
  - Any other text – a custom attribute.
- `DisplayName` – text that is displayed when editing the attribute in MyID.
- `OID` – The attribute OID or name.
- `Encoding` – identifies how the attribute is encoded in the certificate:
  - One of the following ASN1 coding types:
    - `bool`
    - `octet`
    - `int`
  - Any other text – a prefix that is added to the attribute value.
  - Not specified – defaults to using the passed-in attribute text value.

Note: Use of this configuration file is mandatory when setting up certificate policies on PIV systems – PIV requires the use of attribute mapping – but you can also use attribute mapping on non-PIV systems.

2.4.1 Example configuration file

For example:

```
<Extensions>
    <Extension>
        <Name>NACI</Name>
        <DisplayName>NACI</DisplayName>
        <OID>2.16.840.1.101.3.6.9.1</OID>
        <Encoding>{bool}</Encoding>
    </Extension>
    <Extension>
        <Name>san</Name>
        <DisplayName>RFC 822 Name(E-mail address)</DisplayName>
        <OID>Email</OID>
    </Extension>
    <Extension>
        <Name>san</Name>
        <DisplayName>Uniform Resource ID</DisplayName>
        <OID>UUID</OID>
        <Encoding>urn:uuid:</Encoding>
    </Extension>
    <Extension>
        <Name>san</Name>
        <DisplayName>User Principal Name</DisplayName>
        <OID>1.3.6.1.4.1.311.20.2.3 </OID>
    </Extension>
    <Extension>
        <Name>san</Name>
        <DisplayName>FASC-N (Hex)</DisplayName>
        <OID>2.16.840.1.101.3.6.6 </OID>
        <Encoding>{octet}</Encoding>
    </Extension>
</Extensions>
```

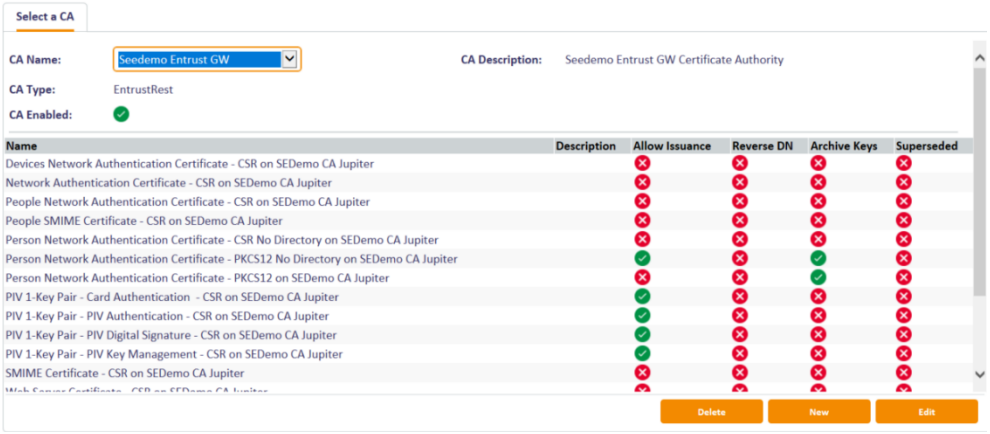
The following policy attributes are defined in the above example:

- A PIV NACI attribute that is encoded as an ASN1 `bool`.
- A `san` email attribute encoded as a text string (no `Encoding` is specified).
- A `san` Uniform Resource ID that is prefixed by `urn:uuid:`
- A User Principal Name encoded as a text string.
- A `san` FASC-N (HEX) that is encoded as an ASN1 `octet`.

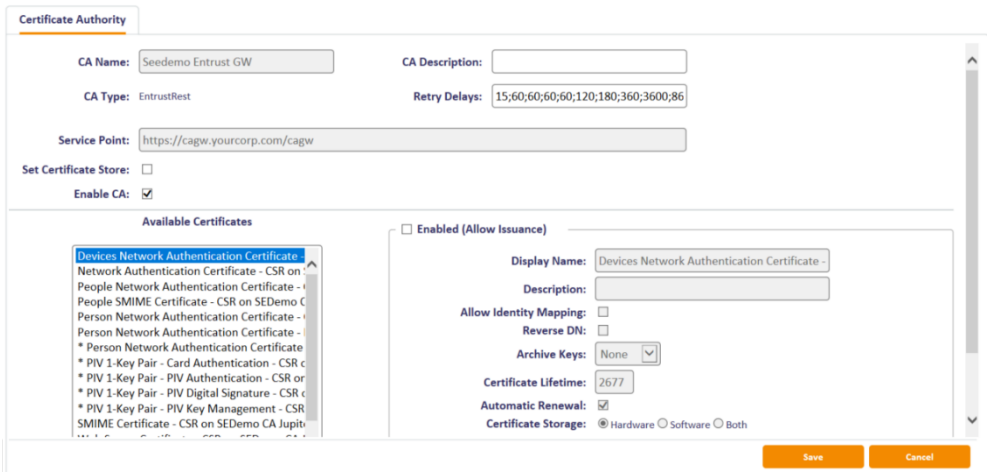
2.5 Enabling certificate policies

Although all certificate policies are detected when you add the CA to MyID, they are all initially disabled. To enable them:

1. From the **Configuration** category, select **Certificate Authorities**.
2. From the **CA Name** drop-down list, select the certificate authority you want to work with.



3. Click **Edit**.



4. Make sure **Enable CA** is selected.
5. Select a certificate template you want to enable for issuance within MyID in the **Available Certificates** list.
6. Click the **Enabled (Allow Issuance)** checkbox.
7. Set the options for the policy:
   - **Display Name** – the name used to refer to the policy.
   - **Description** – a description of the policy.
   - **Allow Identity Mapping** – used for additional identities. See the *Additional identities* section in the ***Administration Guide*** for details.
   - **Reverse DN** – select this option if the certificate requires the Distinguished Name to be reversed.

- **Archive Keys** – select whether the keys should be archived.

  See section *2.1*, *Key archival and recovery* for details.
- **Certificate Lifetime** – the life in days of the certificate. You can request a certificate from one day up to the maximum imposed by the CA. For example, type `365` to request one-year certificates.

  Note: The default certificate lifetime value in MyID is 365 days. The default in Entrust is 36 months; if you want to configure MyID to match the Entrust default, enter 1095 days.
- **Automatic Renewal** – select this option if the certificate is automatically renewed when it expires.
- **Certificate Storage** – select one of the following:
  - **Hardware** – the certificate can be issued to cards.
  - **Software** – the certificate can be issued as a soft certificate.
  - **Both** – the certificate can be issued either to a card to as a soft certificate.
- **Recovery Storage** – select one of the following:
  - **Hardware** – the certificate can be recovered to cards.
  - **Software** – the certificate can be recovered as a soft certificate.
  - **Both** – the certificate can be recovered either to cards or to a soft certificate.
  - **None** – allows you to prevent a certificate from being issued as a historic certificate, even if the **Archive Keys** option is set. If the **Certificate Storage** option is set to **Both**, the certificate can be issued to multiple credentials as a shared live certificate, but cannot be recovered as a historic certificate.
- Additional options for storage:

  If you select **Software** or **Both** for the **Certificate Storage**, or **Software**, **Both**, or **None** for the **Recovery Storage**, set the following options:
  - **CSP Name** – select the name of the cryptographic service provider for the certificate. This option affects software certificates issued or recovered to local store for Windows PCs.

    The CSP you select determines what type of certificate templates you can use. For example, if you want to use a 2048-bit key algorithm, you cannot select the Microsoft Base Cryptographic Provider; you must select the Microsoft Enhanced Cryptographic Provider. See your Microsoft documentation for details.
  - **Requires Validation** – select this option if the certificate requires validation.
  - **Private Key Exportable** – when a software certificate is issued to local store, create the private key as exportable. This allows the user to export the private key as a PFX at any point after issuance.

    It is recommended that private keys are set as non-exportable for maximum security.

    Note: This setting affects only private keys for software certificates – private keys for smart cards are never exportable.

- **User Protected** – allows a user to set a password to protect the certificate when they issue or recover it to their local store.

  This means that whenever they want to make use of the soft certificate, they will be prompted for a password before they are allowed to use it. This is a CSP feature that is enabled when you set this option, and affects only software certificates that are issued or recovered to local store for Windows PCs.

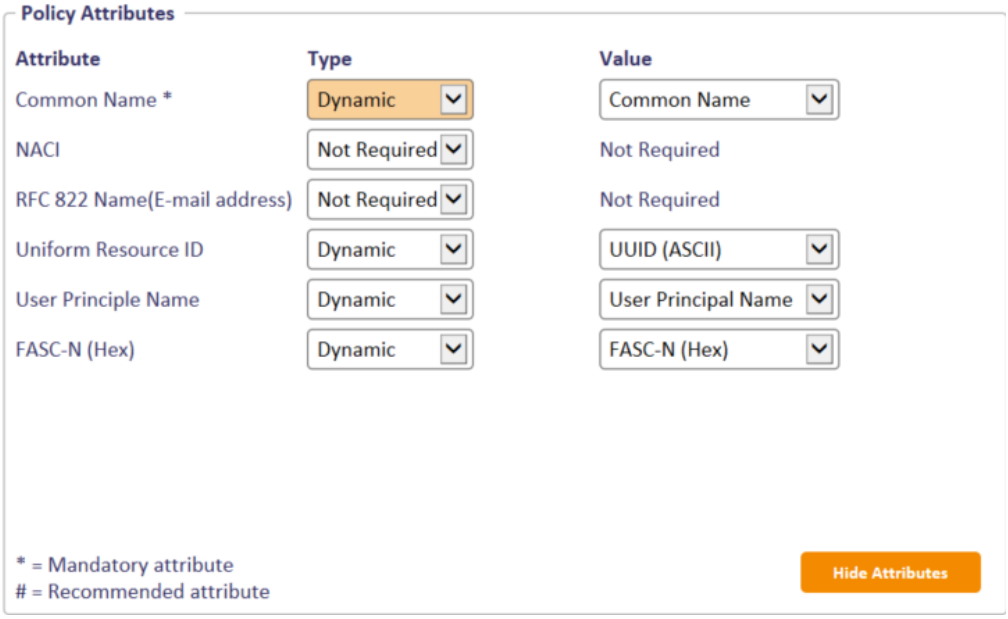
- **Key Algorithm** – select the type and length of the key-pairs used for certificate generation. A longer key length is more secure but certain manufacturers' CSPs do not support longer lengths. Select the appropriate key length from the list. This must match the key type and length set up in your CA.

  Select an RSA type. ECC types are not supported with Entrust CA in this version of MyID.

- **Key Purpose** – select one of the following:
  - **Signature** – the key can be used for signing only.
  - **Signature and Encryption** – the key can be used for either signing or encryption.

  Note: The **Key Purpose** option has an effect only where the device being issued supports the feature. PIV cards do not support this feature, while smart cards issued with minidrivers and software certificates issued to local store for Windows PCs do support this feature.

8. If you need to edit the policy attributes, click **Edit Attributes**.



   a. For each attribute, select one of the following options from the **Type** list:
      - **Not Required** – the attribute is not needed.
      - **Dynamic** – select a mapping from the **Value** list to match to this attribute.

- **Static** – type a value in the **Value** box.

b. Click **Hide Attributes**.

For information on mapping attributes for PIV systems, see section *2.7*, *Attribute mapping for PIV systems*.

Note: MyID may not override the settings of the CA. You need to obtain the correct settings from the administrator of your CA.

9. Click **Save**.

Note: Changes made to certificate profiles do not take effect immediately, as the normal interval for MyID to poll for updates is 50 minutes. To force MyID to poll for changes immediately, you must manually restart the **eKeyServer** service, then restart the **eCertificate** service.

2.5.1 Configuring certificate DN attributes

Important: When issuing non-key archive certificates, the Entrust CA may use the DN from the following for configuring the certificate DN attributes:

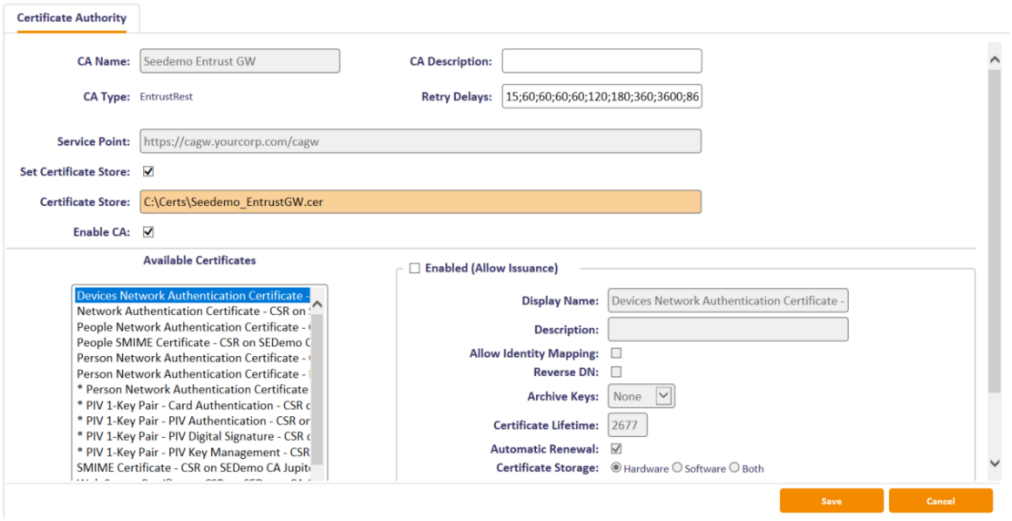
- DN attributes provided in the certificate request.
- DN from the provided CSR in the certificate request.

The Entrust CA will prioritize the use of the DN in the certificate request with the DN from the CSR being used if the DN is not provided in the request. As such, where the requirement is that the DN provided in the CSR is used for a given policy, the DN attributes must not be configured for that certificate policy.

2.6 Updating CA details

You can edit the authentication certificate location and enable or disable the CA.

1. From the **Configuration** category, select **Certificate Authorities**.
2. From the **CA Name** drop-down list, select the certificate authority you want to work with.
3. Click **Edit**.



4. Enable or disable the **CA** by selecting or deselecting the Enable CA checkbox.
5. To change the certificate location, ensure that the Set Certificate Store checkbox is selected, the update the certificate location as described in section *2.3*, *Set up the MyID Entrust certificate authority*.
6. Click **Save**.

2.7 Attribute mapping for PIV systems

For PIV systems, you must set up the attributes of the PIV certificate policies to have specific dynamic mappings.

Note: The FASC-N mapping is required for standard PIV cards, but is not permitted for PIV-I cards. The PIV Card Authentication certificate policy *must not* contain a mapping for Email.

2.7.1 Example attribute mapping for PIV systems

Certificate Policy	FASC-N	UUID	NACI	User Principal Name	Email
PIV Authentication	FASC-N (Hex)	UUID (ASCII)	NACI Status	User Principal Name	Not Required
PIV Card Authentication	FASC-N (Hex)	UUID (ASCII)	NACI Status	Not Required	Not Required
PIV Encryption	Not Required	Not Required	Not Required	Not Required	Email (optional)
PIV Signing	Not Required	Not Required	Not Required	Not Required	Email (optional)

2.7.2 Example attribute mapping for PIV-I systems

Certificate Policy	FASC-N	UUID	NACI	User Principal Name	Email
PIV Authentication	Not Required	UUID (ASCII)	Not Required	User Principal Name	Not Required
PIV Card Authentication	Not Required	UUID (ASCII)	Not Required	Not Required	Not Required
PIV Encryption	Not Required	Not Required	Not Required	Not Required	Email (optional)
PIV Signing	Not Required	Not Required	Not Required	Not Required	Email (optional)

2.7.3 Editing the attribute mappings

To edit the attribute mapping:

1. Within the **Certificate Authorities** workflow, select an enabled certificate policy.
2. Click **Edit Attributes**.
3. For each attribute, select one of the following options from the **Type** list:
   - **Not Required** – the attribute is not needed.
   - **Dynamic** – select a mapping from the **Value** list to match to this attribute.
   - **Static** – type a value in the **Value** box.
4. Click **Save**.

2.8 Limitations

The following are known limitations with MyID's integration with an Entrust CA accessed through the Entrust CA Gateway:

- MyID has not been tested with Entrust CA policies that have been configured to support ECC keys and related signing algorithms.
- The Entrust CA Gateway API does not support directory certificate attributes.
- The Entrust DN tracking feature is not currently supported by the MyID Entrust Rest API connector.

3 Logging

You can set up logging for the Entrust Rest API connector component, which may provide additional information if the error details from the response from the Entrust CA Gateway does not provide enough information to diagnose your issues.

To set up logging for the component:

1. Set the following in the application server's registry:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Intercede\Edefice\Trace`

   If the `Trace` key does not exist, you must create it.

2. In the `Trace` key, create a DWORD value called `EntrustRestConnector`. Set the value to `1` to enable logging, and `0` to disable logging.

3. In the `Trace` key, create a key called `EntrustRestConnector`. Within this key, create a string value called `Location` and set this to the full path of the file to which you want to send the log information.

   Note: You must ensure that the MyID named COM user has the necessary permissions to create and write to the log file. You can create a file then give the user write permissions if you prefer not to give the user create permissions.

Important: Disable the logging when you have completed diagnosing the issues, as the log file may become very large.