LA-UR-16-21404
Approved for public release; distribution is unlimited.

Title: PIV Logon Configuration Guidance

Author(s): Lee, Glen Alan

Intended for: Report

Issued: 2016-03-04

PIV Logon Configuration Guidance

Version 1.0
February 29, 2016

Network and Infrastructure Engineering Division
Core Services Group (NIE-CS)
Los Alamos National Laboratory

Contents

Revision History

Version	Date	Comment
1.0	2016FEB29	• Initial version of document that describes configuration guidance for implementing PIV Logon based on lessons learned at Los Alamos National Laboratory (LANL)

1 Introduction

1.1 Purpose

This document details the configurations and enhancements implemented to support the usage of federal Personal Identity Verification (PIV) Card for logon on unclassified networks.

The guidance is a reference implementation of the configurations and enhancements deployed at the Los Alamos National Laboratory (LANL) by Network and Infrastructure Engineering – Core Services (NIE-CS).

1.2 Intended Usage

This document is intended for network administrators and information technology (IT) staff responsible for maintaining the unclassified network environments.

1.3 Background

The PIV Card (referred to as the HSPD-12 Credential in DOE) is the federal identification credential issued to federal employees and contractor employees. It has electronic features that allow it to be used to identify and authenticate people to facilities (i.e., physical access control systems or PACS) and to networks and applications (i.e., logical access control systems (LACS)).

For LACS usage, the PIV Card contains electronic credentials (X.509 Public Key Infrastructure (PKI) keys and certificates) that assert an individual's identity, which can only be accessed using a Personal Identification Number (PIN). The credential holder keeps the PIN private to prevent unauthorized access or potential compromise of their HSPD-12 Credentials. The HSPD-12 Credential ("something you have") and PIN ("something you know") combination is a 2-Factor authentication mechanism that can be used by many commercial network operating systems and applications that use PKI Certificates for authentication. It is federally mandated by both OMB (via M-11-11) and DOE (via DOE Order 206.2) that PIV Card be used for logging onto federal networks (i.e., PIV Logon).

1.4 PIV Cards at DOE

Most DOE personnel are issued are PIV Card (or HSPD-12 Credentials) from the General Service Administration (GSA) Managed Service Office (MSO) USAccess program (USAccess). Individuals who are employees or contractors affiliated with another federal agency (such as DOD or GSA) will have PIV Cards issued by their home agency. DOE Order 206.2 prohibits issuance of PIV Cards to personnel from other Agencies who already possess a credential; therefore, the unclassified networks can be configured using the guidance in this document to allow other government agencies PIV Cards to be used for logon, if there is a logon requirement for the person.

1.5 Network Environment

While this document uses Microsoft Windows Server 2012 R2 (64-bit) as a reference implementation, the guidance in this document applies to networks operating in Microsoft Windows Server 2008 R2 functional Active Directory (AD) environment or later.

1.6 User Logon Experience

Upon making the Windows desktop configurations in this document, the main logon screen presents the user two icons:

- *Other User* icon
- *Insert a smart Card* icon

To logon with:

1. UserID and password (if PIV logon is not enforced for the use), users
    a. **Click** *Other User* icon
    b. **Type** their *username* in the *Username* field
    c. **Type** their *password* in the *Password* field
2. PIV Card and PIN, users:
    a. **Insert** their PIV Card into a smart card reader
    b. **Click** *Insert a smart Card* icon
    c. **Type** their *6-8 digit PIN* of their PIV Card in the *Password* field
    d. **Type** their *username* in the *Username hint* field

1.7 PIV Logon Process

The PIV logon capability is the native logon feature in Active Directory called Smart Card Logon (SCL). SCL is the usage of smart cards (the PIV Card is a smart card) for authentication. The following explains Microsoft's SCL process at a high-level:

1. At the login screen, user inserts their PIV Card into a smart card reader, types in their 6-8 numeric PIN and types in their username.
2. Workstation creates a signed request using the *PIV Authentication Certificate* (a PKI certificate on the PIV Card) and sends the signed request to the Domain Controller (DC).
3. The DC verifies that the *PIV Authentication Certificate* is valid by checking that:
    a. It was issued by a certification authority the AD trusts (e.g., Entrust Managed Services PKI);
    b. It is not expired; and
    c. It has not been revoked by checking the Certification Revocation List (CRL) or using Online Certificate Status Protocol (OCSP), if available.
4. The DC performs a lookup in AD by matching information from the *PIV Authentication Certificate* with an account in the AD forest.
5. The DC sends a digitally signed authorization to the workstation using the DC's own PKI Certificate.
6. The workstation verifies that the DC PKI Certificate is valid.
7. The logon process completes and the user has access to domain resources and privileges authorized for the account.

1.8 Assumptions

1. Initially, the PIV logon capability will be available as optional logon method to the Windows AD.
    a. As the PIV logon capability is rolled out into production, considerations will be made on how and when to enforce the PIV Card for logon.
    b. When enforced, UserID and Password will be disabled for a user and will be available for logon on an exception basis.
2. Initially, only DOE PIV Cards issued by the USAccess will be supported.
    a. Credentials from other agencies will be addressed if there is a requirement to do so.

1.9 Summary

To summarize the baseline configurations and infrastructure enhancements implemented:

- An Only Locally Trusted (OLT) PKI (using a Microsoft's AD Certificate Services (ADCS)) was deployed and configured to support the issuance of Domain Controller (DC) certificates needed for PIV logon to function. (§ 2.1)
- The Active Directory Trust Stores were configured with the requisite CA certificates to support the PIV Card for logon. (§ 2.2)
- PKI certificates were issued to the DCs from the OLT PKI using auto-enrollment. (§ 2.3)
- DCs were configured to ignore the User Principal Name (UPN) encoded on PIV Cards so that *Certificate Mapping* could be used for configuring user accounts for PIV logon. (§ 2.4)
- A robust validation solution was deployed that includes a Local CRL Repository (§ 2.5.2) and validation software (§ 2.5.3) on DCs to minimize the organization's dependency on external entities for logon to the network. (§ 2.5)
- A GPO was created to restrict PIN change (§ 3.2), to enable the logon fields (§ 3.1), and to enable the desired behavior on PIV Card removal (§ 3.2) on all Windows-based computers and servers.
- Smart card readers were connected to computers. (§ 3.3)
- Windows-based computers (not servers) were configured with ActivClient Middleware to enhance the user experience with the PIV Card. (§ 3.4)
- Users' accounts were configured by mapping their PIV Authentication Certificate from their PIV Card using automated tools and scripts. (§ 4.1.2)

2 Active Directory Configurations and Infrastructure Enhancements

2.1 Microsoft Enterprise Certification Authority

To support smart card authentication in a Microsoft Active Directory environment, the Domain Controllers (DCs) require a PKI certificate (see Section 2.3). For this local PKI requirement, an Only Locally Trusted (OLT) Public Key Infrastructure (PKI) was established using Microsoft's Active Directory Certificate Services (ADCS), which is available on Microsoft's Windows Server 2012 R2 server operating system.

The OLT PKI primarily issues PKI certificates to non-person entities (NPE) on the unclassified internal network. NPEs include hardware devices (e.g., computers, servers, routers) and applications (e.g., web servers, databases, online applications). The term "OLT" is used intentionally to reflect that the PKI only trusted and accepted internally to the organization. Therefore, the OLT PKI only issues PKI certificates to NPEs that do not require interoperability and trusted communications with entities external to the organization. This implementation is consistent with DOE Order 206.2, *"Identity, Credential, and Access Management"*:

> *"DOE Elements may implement internal (or local), site-specific PKIs to satisfy local PKI requirements that do not require trust and interoperability outside of site-specific locations."*

As shown in the figure below, the OLT PKI is a two-tiered PKI architecture, which is recommended based on Microsoft and industry best practices, and exists within the Windows AD environment.

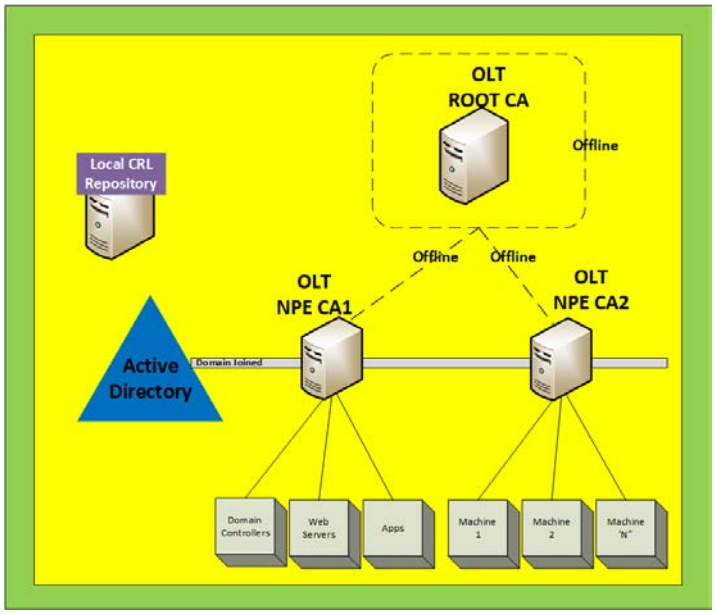
- Tier 1: An offline Root Certification Authority (CA), which only establishes subordinate (or issuing) CAs
- Tier 2: One or more online subordinate CAs in the Windows AD that issue PKI certificates to NPEs

The offline Root CA is hosted on a physical server. When not in use, the Root CA is powered down, and secure in accordance with local procedures.

The subordinate CAs are hosted on Windows virtual machine (VM) servers as members of the Windows AD. One or more subordinate CAs can be established, as needed, to accommodate the various local PKI requirements.

The certificate revocation lists (CRLs) are available via HTTP to the organizations Local CRL Repository (See Section 2.5.2). This allows the OLT PKI to support NPEs that are standalone computers and servers, as well as those that are directly joined (or members) to the Windows AD.

Figure 1: OLT PKI Architecture



All configurations and the concepts for operating and managing the OLT PKI are described in the organization's respective PKI certification practice statement (CPS).

2.2 AD Certificate Trust Stores

The AD Certificate Trust stores must contain the CA certificate chains for the PKI issuers of all certificates involved in the smart card logon process. For the basic implementation to leverage DOE PIV Cards, this includes the CA certificate chains for:

- The OLT PKI (§ 2.1), which issues certificates to the DCs. All domain-joined computers and servers must have the CA chains in their respective trust stores so they "trust" and "validate" the DC certificate during the smart card logon process.
- Entrust Managed Services PKI, which issues the *PIV Authentication Certificate* on DOE PIV Cards.

Table 1 identifies the CA certificate and the GPO configuration[1] to configure the appropriate trust stores for all DCs and all domain-joined Windows computers and servers. As additional PKIs are encountered (such as the DOD PKI for CAC holders), the respective CA certificate chains must be deployed.

Table 1: Certification Authority (CA) Certificates

Certificate Store	CA Certificate	Configuration
Trusted Root Certification Authorities	*Issued to:* ***OLT RootCA*** described in Section 2.1 Notes: • This is the self-signed Root CA for the OLT PKI	Create (or update) GPO by adding (importing) the OLT RootCA to: **Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\Trusted Root Certification Authorities**
Intermediate Certification Authorities	*Issued to:* ***OLT NPE CA1*** described in Section 2.1 *Issued by:* ***OLT RootCA*** Notes: • This is the issuing CA of DC certificates from the OLT PKI	Create (or update) GPO by adding (importing) the OLT NPE CA1 to: **Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\Intermediate Certification Authorities**
Trusted Root Certification Authorities	*Issued to:* ***Entrust Managed Services Root CA*** *Issued by:* ***Entrust Managed Services Root CA*** *Expires:* ***7/23/2025*** *Serial Number:* ***448062f4*** Notes: • This is the self-signed Root CA for DOE PIV Cards issued by GSA USAccess after July 30, 2015 • The cert is posted and maintained at: https://federaladminservices.managed.entrust.com/fedcerts/ • The cross-certificate (issued by Common Policy) is not used in order to eliminate the dependency of accessing external CRLs for all CAs that might be discovered by Microsoft when building the certificate chain to Common Policy	Create (or update) GPO by adding (importing) Entrust Root to: **Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\Trusted Root Certification Authorities** Notes: • See Appendix C.1 for the Base-64 representation of Entrust root to create the ".cer" file for importing

[1] Publishing CA certificates via GPO instead of the certutil command allows for easier removal of CA certs (via GPO) when they are expired or no longer needed. Certutil configures certificates in the registry stores of computers, which requires manual or logon scripts to remove.

Certificate Store	CA Certificate	Configuration
Intermediate Certification Authorities	*Issued to:* ***Entrust Managed Services SSP CA*** *Issued by:* ***Entrust Managed Services Root CA*** *Expires:* ***7/23/2025*** *Serial Number:* ***448063d5*** Notes: • This is the issuing CA of the *PIV Authentication Certificate*, which is the PKI certificate used for PIV Logon with DOE PIV Cards issued by GSA USAccess after July 30, 2015	Create (or update) GPO by adding (importing) Entrust SSP CA to: **Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\Intermediate Certification Authorities** Notes: • See Appendix C.2 for the Base-64 representation of Entrust SSP CA cert to create the ".cer" file for importing
Trusted Root Certification Authorities	*Issued to:* ***Entrust Managed Services Root CA*** *Issued by:* ***Entrust Managed Services Root CA*** *Expires:* ***5/9/2019*** *Serial Number:* ***447f9cf2*** Notes: • This is the self-signed Root CA for DOE PIV Cards issued by GSA USAccess prior to July 30, 2015 • The cert is posted and maintained at: https://federaladminservices.managed.entrust.com/fedcerts/ • The cross-certificate (issued by Common Policy) is not used in order to eliminate the dependency of accessing external CRLs for all CAs that might be discovered by Microsoft when building the certificate chain to Common Policy	Create (or update) GPO by adding (importing) Entrust Root to: **Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\Trusted Root Certification Authorities** Notes: • See Appendix C.3 for the Base-64 representation of Entrust root to create the ".cer" file for importing
Intermediate Certification Authorities	*Issued to:* ***Entrust Managed Services SSP CA*** *Issued by:* ***Entrust Managed Services Root CA*** *Expires:* ***5/9/2019*** *Serial Number:* ***447f9d1f*** Notes: • This is the issuing CA of the *PIV Authentication Certificate*, which is the PKI certificate used for PIV Logon with DOE PIV Cards issued by GSA USAccess prior July 30, 2015	Create (or update) GPO by adding (importing) Entrust SSP CA to: **Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\Intermediate Certification Authorities** Notes: • See Appendix C.4 for the Base-64 representation of Entrust SSP CA cert to create the ".cer" file for importing

To view certificates after the GPO is applied either use:

1. The **certutil** command from any domain-joined computer
    a. *Launch* the **Command** tool
    b. For Trusted Root Certification Authorities:
        i. *type* **certutil –viewstore -grouppolicy root**
    c. For Intermediate Certification Authorities:
        i. *type* **certutil –viewstore -grouppolicy ca**
2. The Windows Certificate Store on any domain-joined computer
    a. *Launch* **MMC**
    b. *Add* **Certificates** snap-in (for local computer)
    c. *Right-click* on **Certificates – Local Computer**

d. *Select* **View| Options**
e. *Check* the box labeled: **Physical Certificate Stores** and *click* **OK** button
f. For Trusted Root Certification Authorities:
    i. *navigate to* **Certificates – Local Computer | Trusted Root Certification Authorities | Group Policy | Certificates**
g. For Intermediate Root Certification Authorities:
    i. *navigate to* **Certificates – Local Computer | Intermediate Certification Authorities | Group Policy | Certificates**

2.3 Domain Controller (DC) Certificates

While a third party CA[2] may be used to issue PKI Certificates to DCs, using the OLT PKI and enabling auto-enrollment ensures that the DC has a valid certificate at all times. As the DC's PKI certificate expires, a new certificate is automatically provisioned by the OLT PKI via auto-enrollment.

In the Windows AD, DCs obtain their PKI certificates from the issuing CA of the OLT PKI, (e.g., *OLT NPE CA1 per* § 2.1), via auto-enrollment. The auto-enrollment setting for the **Default Domain Controller Policy** GPO was updated for DCs[3]:

1. *Logon* to a DC as a member of **Domain Admins** or **Enterprise Admins.**
2. *Click* **Start** | **Administrative Tools** | **Group Policy Management**.
3. In the console tree, *double-click* **Group Policy Objects** in the forest and domain containing the **Default Domain Controller Policy** GPO.
4. *Right-click* the **Default Domain Controller Policy** GPO, and then click **Edit**.
5. *Navigate* to **Computer Configuration | Polices | Windows Settings | Security Settings | Public Key Policies**.
6. *Double-click* **Certificate Services Client - Auto-Enrollment**.
7. *Select* the **Enroll certificates automatically** check box to enable auto-enrollment. Also select:
    - **Renew expired certificates, update pending certificates, and remove revoked certificates** enables auto-enrollment for certificate renewal, issuance of pending certificate requests, and the automatic removal of revoked certificates from a user's certificate store.
    - **Update certificates that use certificate templates** enables auto-enrollment for issuance of certificates that supersede issued certificates.
8. *Click* **OK** to accept changes.

Once auto-enrollment policy is configured, a certificate is issued when there is an auto-enrollment pulse from the DC, which occurs every 8 hours. To force the auto-enrollment to pulse on a DC:

1. *Open* **Command** window
2. *Type* **gpupdate /force**
3. *Type* **certutil –pulse**
4. *Type* **certutil -viewstore my** to verify certificate was issued to the DC

[2] DC PKI Certificate Requirements: http://support.microsoft.com/kb/291010
[3] Configure Certificate Auto-enrollment: http://technet.microsoft.com/en-us/library/cc731522.aspx ***Correction: must be Computer Configuration not User Configuration as stated in TechNet article***

2.4 DC Configuration for Certificate Mapping

To support *Certificate Mapping* using the DOE PIV Cards, The *Default Domain Controllers* GPO was modified to include the registry modifications described in Table 2 so that it is applied to all Windows AD controllers.

Table 2: Domain Control Registry Modification for Certificate Mapping

Registry	Comment
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kdc DWORD: **UseSubjectAltName** Value: **0**	The registry modification is necessary so that the DC ignores the User Principal Name (UPN) that is configured in the Subject Alternate Name (SAN) of all current *PIV Authentication Certificates.*

This guidance is exclusively implementing *Certificate Mapping*, which will require users to enter their username in the *username hint* field that is exposed on the logon interface (see §3.1). The difference that users will see is that the *PIN* field is displayed on top of the *username hint* field; therefore, unlike with username and password, users must enter their PIN first and then their username.

This registry change does not prevent *UPN Mapping* from working if it is needed for one or more accounts for whatever reason. Implementing *UPN mapping* for a select few simplifies the overall configuration and the long-term administration of the PIV logon capability.

2.5 Robust Revocation Status Checking Approach

If the DCs are unable to successfully validate a PIV Card (i.e., perform a PKI certificate status check via CRL or OCSP), logon fails for the user and any other user who attempts to logon to the Windows AD. For an initial pilot implementation of the PIV logon capability, the firewall rules might be modified to allow DCs outbound access to the certificate status information (i.e., CRLs and OCSP) for validating DOE PIV Cards; however, the long-term impact is that the DCs are directly dependent on external entities (e.g. Entrust Managed Services) for availability and sustainability of authentication to the network. Thus, a robust revocation status checking solution was implemented that:

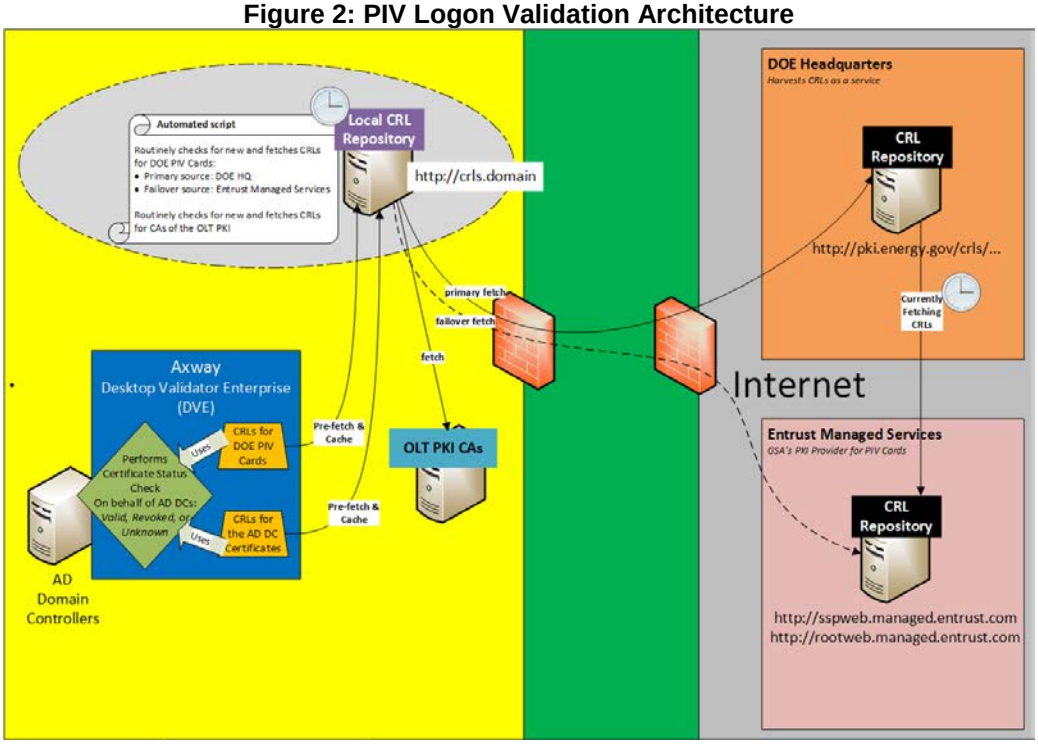
- Offers more autonomy so that organization is less dependent on external entities for the day-to-day logon operations.
- Provides more security to the DCs by no longer requiring firewalls to allow access to external entities.
- Combines the use of CRLs and OCSP and the use of pre-fetching and dynamic querying of revocation data to provide a more fault tolerant validation capability.
- Reduces latency and slowness to the PIV logon process attributed to obtaining revocation data over the WAN/Internet.
- Offers event logging capability that can alert administrators when validation might be failing.
- Provides the ability to quickly deploy contingency configurations for business continuity. Users can continue to logon with PIV Card while administrators diagnose and troubleshoot issues associated with performing revocation status checking within the local infrastructure.

The solution architecture introduces two new components to the local infrastructure:

- An http service that routinely polls for CRLs at the external sources (i.e., http://pki.energy.gov/ and http://managed.entrust.com) and downloads (or caches) them.
- A software agent called, Axway Desktop Validator Enterprise (DVE), which is installed on the Windows AD DCs to augment Microsoft's native capabilities provided via Microsoft CAPI and to perform all of the certificate validation for the DCs.

2.5.1 Concept of Operations

Figure 2: PIV Logon Validation Architecture



The concept of operation (as depicted in Figure 2) is as follows:

1. Entrust Managed Services (*Figure 2, lower right, pink box*) generates the CRLs that required by the DCs to validate (or check the revocation status of) the PKI certificate on the PIV Card that is being used for logon. The CRLs are publicly available and are rather large in size (10+ MB).
2. DOE Headquarters (*Figure 2, upper right, orange box*) harvests CRLs from Entrust and other PKI providers and makes them available via to DOE sites via an http service (http://pki.energy.gov/crls).
3. The Local CRL Repository (*Figure 2, upper left, grey oval*) is an http service that routinely polls DOE HQ, Entrust Managed Services, and the OLT PKI CAs for the latest CRLs.
4. The Axway DVE software (*Figure 2, lower left, blue box*) is installed on DCs and configured (Figure 2, lower left, orange trapezoids in blue box)
    a. To routinely fetch and cache the PIV Card related CRLs from the Local CRL Repository (LCR), which are needed to validate a user's PIV Card during the logon process.
    b. To routinely fetch and cache the CRLs for the OLT PKI CAs, which are needed to validate the DC certificate. Audit records show that the DC attempts to validate its own certificate at least every hour as well as anytime an administrator logs directly onto the DC.
5. When a user initiates a logon with their PIV Card, the DC must perform a revocation status check to ensure the PIV Card is still valid (i.e., not revoked).
    a. The Axway DVE performs the revocation status check (*Figure 2, lower left, green diamond in blue box*) on behalf of the DC, which then continues with the PIV logon process.

2.5.2 Local CRL Repository (LCR)

The Local CRL Repository (LCR) (*Figure 2, upper left, grey oval*) is an http service that stages CRLs for PKIs that the organization may encounter. Initially, the LCR stages only the CRLs that are needed to validate the DOE PIV Cards issued by the GSA USAccess system, which uses the Entrust Managed Services PKI. As the organization encounters other external PKIs, whether for logon or other usages, the LCR may be updated to stage those CRLs as well.

The LCR also stages CRLs issued by the OLT PKI. This allows all internal NPEs (computers, servers, applications) to validate certificates issued by the OLT PKI whether they are standalone systems or systems that are directly joined (or members) to the Windows AD.

2.5.2.1 LCR System Configuration

A basic configuration for the LCR is:

- Operating System: Red Hat Enterprise Linux (RHEL) 5.10
- Web Server Platform: Apache 2.4.10
- GNU Wget: used to retrieve CRL files via http from external sources
- cron script: script containing wget commands that is executed as a cron job

2.5.2.2 LCR Script

An automated script using GNU Wget commands is scheduled as a cron job to download and cache CRLs locally to the LCR. Though the script has additional logic for efficiencies, the pertinent commands to obtain the CRLs are in the following format:

```
export http_proxy=< proxy server if one exists>
wget -nv -N <http URL of target CRL> -P /var/www/html/<folder on local web
service> -a /var/log/<log file name> -nd
```

The script must pull CRLs for the DOE PIV Cards that have PKI Certificates issued by Entrust Managed Services. The primary source of the CRLs is DOE HQ. If the DOE HQ source is unavailable, the script fails over to Entrust. The URLs for the target CRLs are listed in Appendix E.

As additional PKIs are encountered, the URLs for the target CRL(s) that are issued by each PKI will be added to the script. The script is run as a cron job that executes periodically. CRLs are only downloaded if the CRL file on the target system (at DOE HQ or Entrust) is newer than what exists on the LCR. By polling at a high frequency, organization has the freshest CRL data internally.

The automated script also pulls CRLs from the online issuing CAs of the OLT PKI. The CRL for the offline Root CA is stored on the issuing CAs so that the script automatically fetches it as the CRL is updated.

2.5.3 Axway Desktop Validator Enterprise (DVE)

Axway DVE was formerly known as Tumbleweed DVE. Axway DVE[4] was installed on each DC on the Windows AD. The Axway DVE is configured

1. With the *Standard Configuration*, which is fully documented in Appendix F.3
2. Such that revocation status checking is internalized within the local network enclave by utilizing the Local CRL Repository (LCR) (Section 2.5.2) for CRLs
3. To perform revocation status checks only on PKI certificates issued by PKI issuers (i.e., CAs) that the DC is expected to encounter, which include:
    a. The CAs for the Entrust Managed Services PKI, which issues PKI certificates on DOE PIV Cards
    b. The CAs for the OLT PKI, which issues the Windows AD Controller certificates

As other PKIs are encountered (e.g., if another Agency's PIV Card will be used for logon), the DVE will be updated with the relevant CA and revocation information[5].

[4] DVE is for servers such as Domain Controllers, whereas DV is for individual desktops and computers

[5] For any CA that is not configured in the DVE, an audit log will be generated in the Event Viewer application log called, Tumbleweed, for any revocation status check attempted on a PKI certificates issued by that CA

2.5.3.1 Specifications

- Axway DVE version: 4.12.0.127 (64-bit Service Pack 4)
- Windows AD DC operating system: Microsoft Windows Server 2012 R2 (64-bit)

2.5.3.2 DVE Deployment

For the initial install and configuration of DVE on each DC:

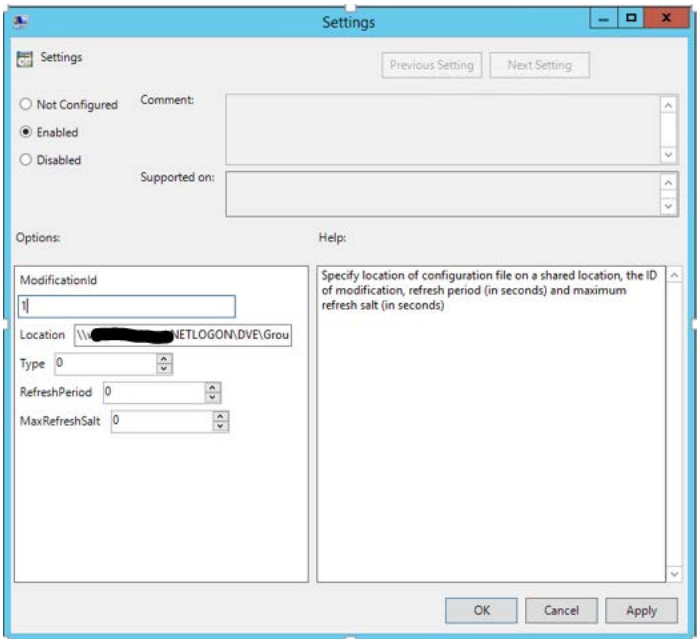
1. *Logon* to **DC**
2. *Install* **DVE** using vendor installation
3. *Configure* **DVE** with the ***Standard Configuration*** *(*Appendix F.3) by.
a. *Launch* **Axway Desktop Validator** console from desktop icon
b. *Select* the **DVE Import / Export** tab
c. *Navigate* to the manual configuration file for the ***Standard Configuration*** listed in Table 4
4. *Reboot* DC
5. *Verify* the DVE configuration was applied by:
    a. *Launching* the **Axway Desktop Validator** console from desktop icon
    b. *Selecting* tabs and comparing to images documented in Appendix F.3.

2.5.3.3 Group Policy Object for DVE

The DVE configuration on DCs is maintained via Group Policy; therefore a Group Policy Object (GPO) [6], (e.g., *Axway_DVE_Configuration_for_DCs)*, was stabled to manage the configurations on the DCs.

The *Axway_DVE_Configuration_for_DCs* GPO uses properly formatted DVE Group Policy configuration files to apply the configurations to DCS. A recommended *Standard Configuration* as well as several contingency configurations are documented in Appendix F along with Table 4, which identifies where the configuration files are stored in the Windows AD for the *Axway_DVE_Configuration_for_DCs* GPO to consume.

Any changes to the *Standard Configuration* are propagated via Group Policy. Additionally, DCs can be configured within minutes[7] with the one of the contingency configurations in order to support business continuity whenever issues occur that are associated with revocation status checking. Appendix F.7 provides guidance on when to apply the various contingency options.



Anytime a DVE configuration needs to be propagated to all the DCs:

1. *Open/Edit* the GPO called, ***Axway_DVE_Configuration_for_DCs***
2. *Navigate* to **Computer Configuration/Policies/Administrative Templates (…)/Classic Administrative Templates (ADM)/DESKTOP VALIDATOR/Configuration**

[6] Instructions for generating properly formatted DVE Group Policy configuration files are in Appendix E

[7] DCs pulse for Group Policies every five minutes, thus all DCs will be configured/updated within five minutes of updating the GPO.

3. *Double-click* the **Settings** object and then
   a. *Select* the **Enabled** radio button
   b. In **ModificationId** field, *increment* the number by 1 from the previous number (**failure to do so will cause the GPO to not be applied to the DCs**)
   c. *Type* the **Universal Name Convention (UNC) locator** of the Group Policy file of the desired configuration in Table 4
   d. *Verify* **zero (0)** is in the fields labeled **Type**¸ **RefreshPeriod***, and* **MaxRefreshSalt**
4. *Click* **Okay** to finish edits
5. *Right-click* on ***Axway_DVE_Configuration_for_DCs*** and *select* ("check") **Link Enabled** to apply the GPO to the DCs

Within 5 minutes, the configurations will be applied to all DCs, since DCs check for GPs every five minutes by default. On each DC, an audit log will be generated in the Event Viewer application log called, Tumbleweed:
Information Event ID 1, System Message: Configuration was successfully reloaded.

3 Microsoft Windows Client Configurations

The configurations in this section are specific to Windows-based computers, servers and virtual machines used by people to authenticate to the Windows AD. This includes Windows 7 (or later) and Windows Server 2008 R2 (or later) platforms. Other platforms (e.g., MAC, Linux) and devices (e.g., tablets, mobile) will be addressed separately when solutions have been vetted.

3.1 Client Registry and/or Local Computer Policy Settings

A GPO (e.g. *PIV_Client_Config*) was created (or updated) and subsequently linked and enforced to all Windows-based computers and servers. The GPO contains the settings that are described in Table 3.

Table 3: Configurations for Windows

Group Policy Object (GPO)	Registry	Comment
Computer Configuration\Policies\Administrative Templates\Windows Components\Smart Card Setting: **Force the reading of all certificates from the smart card** Value: **Enabled**	**HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\SmartCardCredentialProvider** DWORD: **ForceReadingAllCertificates** Value: **1**	This is needed so the PIV Card can be used for logon via *Certificate Mapping*
Computer Configuration\Policies\Administrative Templates\Windows Components\Smart Card Setting: **Allow user name hint** Value: **Enabled**	**HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\SmartCardCredentialProvider** DWORD: **X509HintsNeeded** Value: **1**	This changes the interactive logon screen with a field that allows a user to type the username of the account that they want to logon to as described in § 1.6.
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options Setting: **Interactive logon: Smart card removal behavior** Value: **No Action**	**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon** DWORD: **ScRemoveOption** Value: **0**	• Allows users to replace their badge into their badge holder and remain working at their computer • Allows users to logon with their PIV to multiple computers and use them simultaneously • Complies with DOE/NSSA policy that the badge must be worn and displayed above the waist at all times

Group Policy Object (GPO)	Registry	Comment
User Configuration\Preferences\Windows Settings\Registry	**HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Outlook\RPC** DWORD: **EnableSmartCard** Value: **1**	Outlook 2010 registry modification, described in KB2597028[8] that has addressed an issue experienced by some organizations where user accounts were being locked out upon enforcing PIV logon. Upon opening Outlook, Microsoft Exchange continuously prompted users for domain credentials (username and password), which caused the user's account to lock. Upon applying this registry setting, accounts were no longer being locked out.
User Configuration\Preferences\Windows Settings\Registry	**HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\RPC** DWORD: **EnableSmartCard** Value: **1**	Outlook 2013 registry modification, described in KB2597028[9] that has addressed an issue experienced by some organizations where user accounts were being locked out upon enforcing PIV logon. Upon opening Outlook, Microsoft Exchange continuously prompted users for domain credentials (username and password), which caused the user's account to lock. Upon applying this registry setting, accounts were no longer being locked out.
Computer Configuration\Preferences\Windows Settings\Registry	**HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\SmartCardCredentialProvider** DWORD: **AllowSmartCardPinChangeAndUnblock** Value: **0** if ActivClient is not installed **1** if ActivClient is installed	Needed to support Microsoft Hotfix (see 3.2) Prevents users from being able to change their PIN via the password/pin change option provided by Windows interface. PIN Changes are only allowed if ActivClient is installed, which does enforce the FIPS 201 requirements for PINs.

[8] Microsoft Outlook Hotfix: https://support.microsoft.com/kb/2829595/en-us
[9] Microsoft Outlook Hotfix: https://support.microsoft.com/kb/2829595/en-us

Group Policy Object (GPO)	Registry	Comment
Computer Configuration\Preferences\Windows Settings\Registry	**HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\SmartCardCredentialProvider** REG_SZ: **SmartCardPinChangeAndUnblockString** Value: if ActivClient is not installed: **PIN changes are not allowed from this computer** if ActivClient is installed: **PIN changes are allowed from this computer**	Needed to support Microsoft Hotfix (see 3.2) Message displayed to users who try to change their PIN via the password/pin change option provided by Windows interface.

3.2 Microsoft Hotfix for PIN Changes

The Microsoft hotfix[10], KB#: 2808693, was deployed, along with the associated registry settings in the *PIV_Client_Config* GPO to all Windows-based computers and servers. This prevents users from changing their PIN to a non-PIV conformant PIN. If the GPO detects that the ActivIdentity ActivClient Middleware is installed (Section 3.4), the GPO configures the computer to allow PIN changes since the middleware enforces the PIN policy requirements.

3.3 Smart Card Readers

There are several smart card reader options, which include those that:

- Sit on a desk and plug into a USB port
- Are portable (foldable) and plug into a USB port, when needed
- Are integrated (or built-in) to the keyboard
- Are integrated (or built-in) to laptops

The following are some of smart card readers on the GSA's FIPS 201 Approved Products List (APL) and are being used in DOE; however the table does not reflect all readers that are being used:

Smart Card Reader Type	Name	Comment	Image
External USB Reader	OMNIKEY® 3121 USB Desktop Reader - HID Global APL# 148	Smart card reader that sits on the desk and plugs into a USB port on a computer or laptop.	
External USB Reader	SCR3311 Heavy Weight USB Smart Card Reader (Discontinued) APL#: 51	Smart card reader that sits on the desk and plugs into a USB port on a computer or laptop.	
Keyboard Reader (standard)	Dell KB813 Smartcard USB Keyboard APL#: 1186	Smart card reader is built-in the keyboard for convenience. Dell Keyboards **only when included** with some standard Dell desktop and workstation computers.	

[10] PIN Change Hotfix: http://support.microsoft.com/kb/2808693

Smart Card Reader Type	Name	Comment	Image
Keyboard Reader (standard)	CHERRY G83-6644 FIPS 201 Certified Smart Card Keyboard APL#: 325	Smart card reader is built-in the keyboard for convenience.	
Laptop Integrated Reader	Dell & HP laptops	Smart Card Readers have been included in most standard laptops for several years and are typically found on the side of laptop. Dell: Drivers may be required HP: Drivers may be required	
Portable (Foldable) USB Reader	CLOUD 2900 R SCR3500A APL#: 1262	Smart card reader plugs into a USB port on a computer or laptop. Is designed to be portable and easy to transport.	
Portable (Foldable) USB Reader	SCM SCR3500 (Discontinued) APL#: 463	Smart card reader plugs into a USB port on a computer or laptop. Is designed to be portable and easy to transport. This is the reader has been used in the past but the version has been discontinued and is no longer available for purchase.	

3.4 PIV Middleware

Though Microsoft Windows 7 (and later) include a native Microsoft smart card mini-driver[11] that allows the PIV Card to work for PIV logon, many organizations have decided to configure PIV Middleware on Windows-based computers to enhance the overall user experience with the PIV Card. Though there are alternatives on the GSA FIPS 201 Approved Products List (APL), many organizations are using ActivIdentity ActivClient 7 on Windows-based computers.

3.4.1 Deployment

Organizations can establish an installation package which can be deployed using SCCM or an application catalog. The vendor documentation provides guidance on how to create the installation package.

3.4.2 Installation Package

The installation package ensures that the steps described in Section 3.4.3 are performed to successfully install ActivClient in a manner that

- Automatically configures Firefox to use the PIV Card
- Prevents incompatibility with Entrust software on desktops
- Installs the appropriate ActivClient features needed for users
- Removes ActivClient features that will cause conflicts with Entrust or are not applicable to organization
- Applies the latest hotfix for the ActivClient software

[11] Smart Card Enhancements: http://technet.microsoft.com/en-us/library/ff404304(v=ws.10).aspx

3.4.3 Configuration

The ActivClient middleware settings on Windows-based computers can be configured and managed via Group Policy Object (GPO). It is recommend to create or update an existing GPO (e.g., *PIV_Client_Config* previously referenced in this document) that contains all PIV Card related configuration settings. The ActivIdentity ActivClient Group Policy templates are used in the GPO.

3.4.4 Manual Installation

To install the ActivIdentity Middleware without the installation package described in Section 3.4.2, the following must be done in order:

1) *Copy* the following **files** to a local directory (e.g., c:\temp) on the target computer
   a) For 32-bit Windows platforms
      i) ActivClient x86 7.0.2.msi
      ii) The latest hotfix (*.msp) from the vendor
   b) For 64-bit Windows platforms
      i) ActivClient x64 7.0.2.msi
      ii) The latest hotfix (*.msp) from the vendor
2) *Verify* **Mozilla Registry value** exists (or create if necessary),:
   a) For 32-bit Windows platforms: "HKLM\SOFTWARE\Mozilla\Mozilla Firefox" /v CurrentVersion /t REG_SZ /d "31.6.0"
   b) For 64-bit Windows platforms: "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Mozilla\Mozilla Firefox" /v CurrentVersion /t REG_SZ /d "31.6.0"
3) *Install* **ActivClient** software
   Note: This is a passive install, which could take a minute or two. The status indicator will disappear when install is complete
   a) For 32-bit Windows platforms
      i) *Launch* a **Command** window as administrator
      ii) *Type* (or copy): cd c:\temp
      iii) *Type* (or copy) the following:
      msiexec /i "ActivClient x86 7.0.2.msi" AddLocal=ALL Remove=Outlook,SettingsManagement,DeptOfDefenseConfiguration /passive /norestart
   b) For 64-bit Windows platforms
      i) *Launch* a **Command** window as administrator
      ii) *Type* (or copy): cd c:\temp
      iii) *Type* (or copy) the following:
      msiexec /i "ActivClient x64 7.0.2.msi" AddLocal=ALL Remove=Outlook,SettingsManagement,DeptOfDefenseConfiguration /passive /norestart
4) *Install* **ActivClient** Hotfix
   Note: This is a passive install, which could take a minute or two. The status indicator will disappear when install is complete
   a) For 32-bit Windows platforms
      i) *Launch* a Command window as administrator
      ii) *Type* (or copy): cd c:\temp
      iii) *Type* (or copy): msiexec /p latest_hotfix.msp /passive /norestart
   b) For 64-bit Windows platforms
      i) *Launch* a Command window as administrator
      ii) *Type* (or copy): cd c:\temp

iii) *Type* (or copy): msiexec /p latest_hotfix.msp /passive /norestart

5) *Reboot*
Note: ActivClient will not be configured or function correctly until computer is restarted after initial install of software

4 User Account Configuration

4.1 Associating PIV Card with Account

This guidance is for organizations using *Certificate Mapping* (vice *UPN Mapping*) to configure accounts on the Windows AD for PIV logon. If *UPN Mapping* is required in the future, each account that uses *UPN Mapping* must also be configured for *Certificate Mapping*; otherwise, logon will fail for these accounts.

Certificate Mapping entails configuring the *altSecurityIdentities* attribute of user's AD account with specific information from the user's PKI certificate being used for authentication. Though Microsoft offers several options for certificate mapping[12], this guidance uses the default configuration option of **Issuer <I>** and **Subject <S>** fields of the user's *PIV Authentication Certificate*.

- Format
  - *altSecurityIdentities:X509:<I>[full DN of issuer]<S>[full DN of subject]*
- Where
  - *[full DN of issuer]* contains the DN information from the Issuer field of the user's certificate
  - *[full DN of subject]* contains the DN information from the Subject field of the user's certificate

- Example: John Smith's PIV Card issued by the GSA USAccess System

```
altsecurityidentities:X509:<I>C=US,O=Entrust,OU=Certification
Authorities,OU=Entrust Managed Services SSP CA<S>C=US,O=U.S.
Government,OU=Department of Energy,CN=JOHN SMITH(Affiliate)
OID.0.9.2342.19200300.100.1.1=89001122334455
```

4.1.1 DOE PIV Card Quirk

There is an anomaly with the PKI certificates issued on DOE PIV Cards via the GSA USAccess system. The OID that is included in the Subject Name is not always consistent from user to user, or from card to card. As shown below, the OID can appear before or after the Common Name (CN).

```
X509:<I>C=US,O=Entrust,OU=Certification
Authorities,OU=Entrust Managed Services SSP CA<S>C=US,O=U.S.
Government,OU=Department of Energy,CN=JOHN SMITH(Affiliate)
OID.0.9.2342.19200300.100.1.1=89001122334455
```

```
X509:<I>C=US,O=Entrust,OU=Certification
Authorities,OU=Entrust Managed Services SSP CA<S>C=US,O=U.S.
Government,OU=Department of
Energy,OID.0.9.2342.19200300.100.1.1=89001122334455 CN=JOHN
SMITH(Affiliate)
```

Therefore, organizations should configure each user account with both versions of the Subject Name so users are not impacted by the anomaly as they get new or updated PIV Cards.

[12] Certificate Mapping options: http://blogs.msdn.com/b/spatdsg/archive/2010/06/18/howto-map-a-user-to-a-certificate-via-all-the-methods-available-in-the-altsecurityidentities-attribute.aspx

4.1.2 Automated Mapping

This section describes a semi-automated process for configuring user accounts on the Windows AD. Using a set of PowerShell scripting tools:

1. A *Master List of PIV Data* is generated and maintained using data from GSA USAccess *Application Status Report (ASR)*. Since the ASR does not contain any identifier that is specifically unique to the organization (e.g., such as site specific employee ID), the PowerShell script performs fuzzy logic using ASR attributes (site name on badge, email address, and naming information) to match to an employee in organization's local LDAP repository. Thus, the *Master List of PIV Data* is registry of PIV Data that is tied to (or associated with) a person's local employee ID.
2. The *altSecurityIdentities* attribute for one or more accounts is updated with the X509 certificate mappings associated with a user's PIV Card using the *Master List of PIV Data* registry.

The process will significantly improve when the NNSA OneID Attribute Exchange Service (AES) is available. The OneID will contain HSPD-12 (or PIV) data that is correlated with organization's employee information; thus, the organization will not have to rely on fuzzy logic for associating an employee with their actual PIV Card. Furthermore, the organization will be able fully automate the updates to the Windows AD accounts since there will be an online authoritative source available in OneID.

4.1.3 Manual Mapping

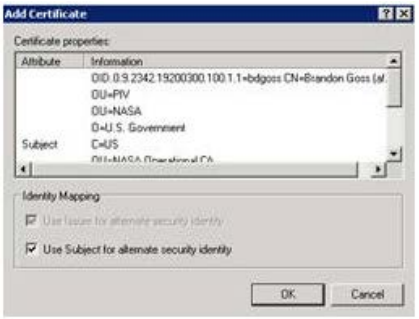
If necessary, the Active Directory Users and Groups (ADUC) tool can be used to configure the *altSecurityIdentities* attribute of a user's account with the *PIV Authentication Certificate*. This is only recommended if the account cannot be configured using the process in Section 4.1.2, such as for PIV Cards for users from other Federal agencies.

To use ADUC, the person's *PIV Authentication Certificate* file (".cer" file) is exported from their PIV Card as described in Appendix D.

> **WARNING!** Configuring accounts with certificates using ADUC ***must be*** done on computers or servers that ***do not*** have Entrust Entelligence Service Provider (ESP) software installed. Testing showed that the presence of the ESP software replaces the string, "OID.0.9.2342.19200300.100.1.1", which is in the *Subject* name of *PIV Authentication Certificate*s to, "UID", when importing using ADUC. Logon will fail unless the *Subject* name in the *altSecurityIdentities* attribute exactly matches what is on the PIV Card.

To configure account for certificate mapping using ADUC:

1. *Launch* **ADUC** from a computer or server that does not have Entrust ESP installed
2. *Right click* on the **user account** and *select* **Name Mappings** from the drop-down menu
3. *Click* **Add** *(button)* and *select* the **PIV Authentication Certificate** file (.cer) to map to the account
4. *Click* **OK** *(button)* to finish.



4.2 Enforcing PIV Card for 2-factor Authentication

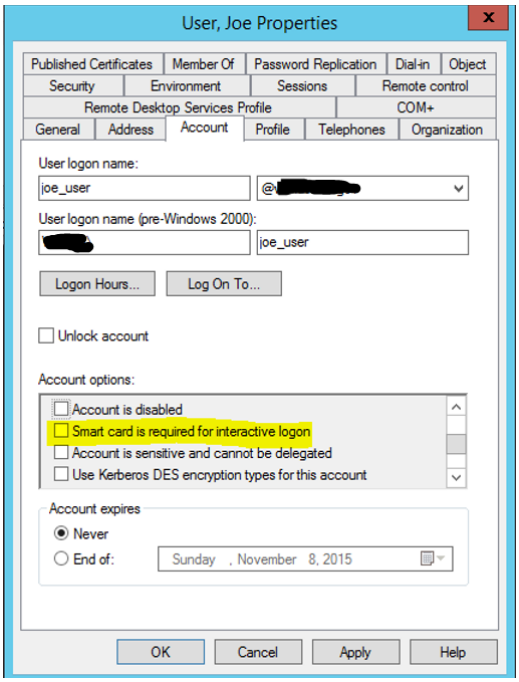
The following describes a process for enforcing 2-factor authentication (2FA) with the PIV Card at the account-level to the greatest extent practical. If needed, alternatives to account-level enforcement will be considered.

Account-level enforcement amounts to configuring the user's account on the Windows AD such that a password can no longer be used by a user to authenticate to the Windows AD or to any resource on the Windows AD that uses Windows AD as its authentication source. User accounts that require knowledge of the Windows AD password in order to perform a mission and/or business function will be temporarily excluded from the 2FA enforcement until the password dependency is addressed.

This section discusses account-level enforcement and the approach to effectively manage how user accounts in the Windows AD are enforced.

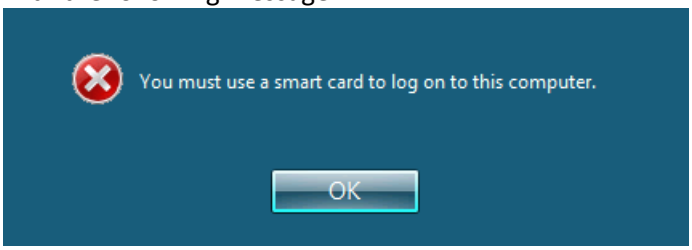
4.2.1 Account-level enforcement

To enforce (or require) the PIV Card for 2-factor Authentication, the AD user account setting *"Smart card is required for interactive logon"* must be enabled (or checked).



If the *"Smart card is required for interactive logon"* is not enabled (no checked) for the AD user account, then the user will be able to continue to logon with username and password (UN/PW). To prevent the user from being able to logon with UN/PW, "require smart card for interactive logon" needs to be selected. Upon doing so, the password is changed to a random 256 character password and UN/PW will no longer be allowed for the AD user account.

If a user tries to logon with UN/PW, they will be presented with the following message:



To allow for UN/PW again, the user account has to be configured and a password reset must be performed.

4.2.2 Managing 2FA enforcement

AD security groups and PowerShell scripts are implemented to effectively manage and enforce 2FA on user accounts on the Windows AD. Using this strategy, an organization can run reports and assess

1. How many user accounts are expected to be using the PIV Card for 2FA
2. How many user accounts are being exempted and whether it is a short-term or a mission need
3. If user accounts exist in the Windows AD but have been omitted from the 2FA requirement

This strategy could be adapted to use with machine-level enforcement as well, for those who are not enforcing 2FA at the account level.

The following provides the high-level approach to managing the 2FA enforcement on the Windows AD:

1. There are a set of 2FA "Required" and "Exemption" security groups in the Windows AD that include:
    a. 2FA_Required: members of this group have the *"Smart card is required for interactive logon"* setting configured unless they are a member of one of the "Exemption" groups.
    b. 2FA_Daily_Exemption: members of this group have been identified as needing a reprieve of the 2FA requirement for the day. This "Exemption" group is cleared on a nightly basis.
    c. 2FA_Short-term_Exemption: members of this group have been identified as needing a reprieve of the 2FA requirement on a short-term duration (e.g., waiting for PIV Card).
    d. 2FA_Mission_Exemption: members of this group include those accounts for users who would be negatively impacted by 2FA enforcement with a PIV Card and have proven they are unable to perform one or more mission or business functions.
2. All user accounts (standard and admin) are members of the 2FA_Required security group, because the underlying premise is that all accounts associated with a user are expected to be using 2FA.
3. A user account is added to the appropriate 2FA "Exemption" security group, as needed.
4. A 2FA-Enforcement PowerShell script, which is scheduled to run nightly (after business hours):
    a. Clears the 2FA_Daily_Exemption security group membership; and
    b. Sets the *"Smart card is required for interactive logon"* setting on each user account (or member) in the 2FA_Required security group unless the user account is in one of the 2FA "Exemption" security groups.

The 2FA "Required" and "Exemption" security groups are managed in the following manner:

1. 2FA_Required:
    a. All user accounts (standard and admin) are members of the 2FA_Required security group, because the underlying premise is that all accounts associated with a user are expected to be using 2FA.
    b. Service accounts or any account that is not associated with a user are not included in the 2FA_Required security group
2. 2FA_Daily_Exemption:
    a. A user account is added to the group whenever a reprieve of the 2FA requirement for the day has been substantiated.
    b. If the 2FA-Enforcement PowerShell script is run during the day, user accounts that are members of this security group will not be configured for 2FA enforcement.
    c. This "Exemption" group is cleared on a nightly basis.
    d. Once the user account is removed from this security group, it will be enforced for 2FA the next time the 2FA-Enforcement PowerShell script is executed, unless the user is a member of one of the other "Exemption" security groups.
3. 2FA_Short-term_Exemption:
    a. A user account is added to the group whenever a short-term (greater than a day) reprieve of the 2FA requirement has been substantiated (e.g., waiting for PIV Card).
    b. Members of this security group only include those who would normally be expected to use their PIV Card for logon if they had it available.
    c. Membership of this security group is assessed often to ensure that the users are only exempted for the amount of time required.
    d. Anytime the 2FA-Enforcement PowerShell script is executed, user accounts that are members of this security group will not be configured for 2FA enforcement.
    e. Once the user account is removed from this security group, it will be enforced for 2FA the next time the 2FA-Enforcement PowerShell script is executed, unless the user is a member of one of the other "Exemption" security groups.

4. 2FA_Mission_Exemption:
    a. A user account is only added to this security group if it is determined that enforcing 2FA would negatively impact their ability to perform one or more mission or business functions.
    b. Membership of this security group is assessed at least every 6 months to determine whether the exemption still is applicable to the user.
    c. When there is evidence that the mission and/or business function is able to support the PIV Card, the respective user accounts will be removed from this group.
    d. Anytime the 2FA-Enforcement PowerShell script is executed, user accounts that are members of this security group will not be configured for 2FA enforcement.
    e. Once the user account is removed from this security group, it will be enforced for 2FA the next time the 2FA-Enforcement PowerShell script is executed, unless the user is a member of one of the other "Exemption" security groups.

During the initial roll-out of the 2FA enforcement with the PIV Card:

1. All user accounts in the Windows AD are
    a. Added to the 2FA_Short-term_Exemption security group; and
    b. Added to the 2FA_Required security group
2. As a group of users are targeted for 2FA enforcement, the respective user account (or accounts if users have multiple) are:
    a. Removed from the 2FA_Short-term_Exemption security group;
    b. Assessed to determine if they warrant an exemption and be added to the appropriate "Exemption" security group;
    c. Enforced with 2FA by executing 2FA-Enforcement PowerShell script, which only enforces 2FA on accounts that are not in one of the "Exemption" security groups
3. The expectation is that the membership of the 2FA_Short-term_Exemption security group will move towards zero as the 2FA requirement is fully implemented.

Short-term, the network or security administrators will routinely scrub the Windows AD for user accounts and add to appropriate 2FA security groups using scripts. Long-term, the organization's account creation and management processes could be enhanced to ensure user accounts are included in the appropriate 2FA security groups.

Appendix A Deployment Anomalies

The following describes anomalies that some encountered when using this guidance for implementing the PIV logon capability.

A.1 Anomaly #1: DCOM GPO impacts issuance of certificates to DC via auto-enrollment from OLT CA.

Observation: The DCs were not getting PKI certificates from the OLT PKI even after ensuring the OLT CA and the auto-enrollment GPO was properly configured.

Resolution: Windows 2012 R2 server hosting the OLT CAs were getting a GPO with a setting that includes the local security policy setting, *DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax*. Certificates were successfully issued to the DCs upon modifying this setting to include **Authenticated Users** with the following set to **Allowed**:

- Local Launch
- Remote Launch
- Local Activation
- Remote Activation

A.2 Anomaly #2: "You cannot use a smart card to log on because smart card logon is not supported for your user account"

Observation: Upon initial implementation, PIV logon was failing initially from both Windows 7 and Windows Server 2008 clients. The following error message was displayed upon the user entering their PIN and username hint:

> *"The system could not log you on. You cannot use a smart card to log on because smart card logon is not supported for your user account. Contact your system administrator to ensure that smart card logon is configured for your organization."*

Resolution: Upon performing extensive research, trying recommendations prescribed by blogs and TechNet articles for this particular error message, and ensuring all configurations were applied as documented, the result was no different. Upon rebooting all DCs in the Windows AD, PIV logon was successful. None of the online documentation for configuring smart card logon in an Active Directory environment indicates a reboot is necessary. In the development environment, PIV logon worked without rebooting the DCs. So the answer remains the same to issues unexplained: "When in doubt, reboot."

Appendix B References

The following is a catalog of references to documents and online articles that were used to identify configurations and/or troubleshoot items when testing and deploying PIV logon in both development and production environments.

#	Title/Article	Location
1.	DOE Smart Card Configuration and Operations Guidance version 3.0	https://spaces.kcp.com/display/doelacs/Domain+Logon.
2.	Microsoft's HSPD-12 Logical Access Authentication and Active Directory Domains	http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=9427
3.	How to disable the Subject Alternative Name for UPN Mapping	http://technet.microsoft.com/fr-fr/library/ff520074(WS.10).aspx
4.	Map a user to a certificate via all the methods available in the altSecurityIdentities attribute	http://blogs.msdn.com/b/spatdsg/archive/2010/06/18/howto-map-a-user-to-a-certificate-via-all-the-methods-available-in-the-altsecurityidentities-attribute.aspx
5.	Mapping one smartcard certificate to multiple accounts	http://blogs.technet.com/b/askds/archive/2009/08/10/mapping-one-smartcard-certificate-to-multiple-accounts.aspx
6.	Certificate Templates Overview	http://technet.microsoft.com/sv-se/library/cc730826(WS.10).aspx
7.	Configure Certificate Auto-enrollment *(Note: TechNet Article Correction: Reference to "User Configuration" in the GPO should be "Computer Configuration")*	http://technet.microsoft.com/en-us/library/cc731522.aspx
8.	Requirements for domain controller certificates from a third-party CA	http://support.microsoft.com/kb/291010
9.	Smartcard logon using certificates from a 3rd party on a Domain Controller and KDC Event ID 29	http://blogs.technet.com/b/instan/archive/2011/05/17/smartcard-logon-using-certificates-from-a-3rd-party-on-a-domain-controller-and-kdc-event-id-29.aspx
10	Guidelines for enabling smart card logon with third-party certification authorities	http://support.microsoft.com/kb/281245
11	Smart Card Enhancements *(PIV mini-driver)*	http://technet.microsoft.com/en-us/library/ff404304(v=ws.10).aspx
12	DC PKI Certificate Requirements if issued by Third Party CA	http://support.microsoft.com/kb/291010
13	Moving Your Organization from a Single Microsoft CA to a Microsoft Recommended PKI	http://blogs.technet.com/b/askds/archive/2010/08/23/moving-your-organization-from-a-single-microsoft-ca-to-a-microsoft-recommended-pki.aspx
14	Remove a Certificate Template from a CA	http://technet.microsoft.com/en-us/library/cc772358.aspx
15	Microsoft Hotfix for PIV PIN Changes from Windows 7 or later and Windows Server 2008 or later	http://support.microsoft.com/kb/2808693
16	Add a Certificate Template to a CA	http://technet.microsoft.com/en-us/library/cc771937.aspx

#	Title/Article	Location
17	Add a Certificate Template to a CA via certutil	http://social.technet.microsoft.com/Forums/windowsserver/en-US/8e7404d5-801e-4ba1-8fbf-709858c91ea4/ca-missing-templates-in-enable-certificate-templates?forum=winserversecurity
18	Removing Domain Controller Certificates	http://technet.microsoft.com/en-us/library/cc783979(v=ws.10).aspx
19	Decommissioning a Microsoft Enterprise CA	http://support.microsoft.com/kb/889250

Appendix C Certification Authority Certificates

C.1 Entrust Managed Services Root CA – Expires 2025

This is the Entrust Root CA certificate for PIV Cards issued after July 30, 2015 by GSA USAccess.

The following Base-64 blob[13] is for:

Issued to: Entrust Managed Services Root CA
Issued by: Entrust Managed Services Root CA
Expires: 7/9/2023
Serial Number: 448062f4

To create a ".cer" file, copy everything from and including "-----BEGIN CERTIFICATE-----" thru "-----END CERTIFICATE-----" into a file with an extension ".cer" (e.g. EntrustRoot2025.cer).

-----BEGIN CERTIFICATE-----
MIIGUDCCBTigAwIBAgIERIBi9DANBgkqhkiG9w0BAQsFADBuMQswCQYDVQQGEwJV
UzEQMA4GA1UEChMHRW50cnVzdDEiMCAGA1UECxMZQ2VydGlmaWNhdGlvbiBBdXRo
b3JpdGllczEpMCcGA1UECxMgRW50cnVzdCBNYW5hZ2VkIFNlcnZpY2VzIFJvb3Qg
Q0EwHhcNMTUwNzIzMTYwNjM2WhcNMjUwNzIzMTYzNjM2WjBuMQswCQYDVQQGEwJV
UzEQMA4GA1UEChMHRW50cnVzdDEiMCAGA1UECxMZQ2VydGlmaWNhdGlvbiBBdXRo
b3JpdGllczEpMCcGA1UECxMgRW50cnVzdCBNYW5hZ2VkIFNlcnZpY2VzIFJvb3Qg
Q0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCYqKN6KNw4zYLKgi6Y
Ooiuw6K/9e/bn7D2gNlAQxPZtGvmvhzIOx2UeHDwhmFkivNy2fgIr85/brQfKguk
WgpcES9Dl2GpcsnOXDSm+cAtGJrEV6/Ecv6o+z2qm0YRODNEaMF4ANLl/H95yfR4
l54aI+MX6rxzTnTv+j/QptL3ZyJe8LnQoeIHr69Jo21e6ekGRtlYJ9L8r5qn7s/b
F9KZ/aksWeB21d1wci3dIIpN5bM8r5YnQLEjjzg35SsbqBEft1/QvgxDbEWTW9/I
Ij5hWrpyBVe23pJwNtEWluvFxhzQz3xJ0U1ZBRQXySVHbx0k0SyRlhhFv6ricooE
ThtJAgMBAAGjggL0MIIC8DCCASAGCCsGAQUFBwELBIIBEjCCAQ4wTwYIKwYBBQUH
MAWGQ2h0dHA6Ly9yb290d2ViLm1hbmFnZWQuZW50cnVzdC5jb20vU0lBL0NBY2Vy
dHNJc3N1ZWRCeUVNU1Jvb3RDQS5wN2MwgboGCCsGAQUFBzAFhoGtbGRhcDovL3Jv
b3RkaXIubWFuYWdlZC5lbnRydXN0LmNvbS9vdT1FbnRydXN0JTIwTWFuYWdlZCUy
MFNlcnZpY2VzJTIwUm9vdCUyMENBLG91PUNlcnRpZmljYXRpb24lMjBBdXRob3Jp
dGllcyxvPUVudHJ1c3QsYz1VUz9jQUNlcnRpZmljYXRlO2JpbmFyeSxjcm9zc0Nl
cnRpZmljYXRlUGFpcjtiaW5hcnkwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E
BAMCAQYwggGIBgNVHR8EggF/MIIBezCB7qCB66CB6IY2aHR0cDovL3Jvb3R3ZWIu
bWFuYWdlZC5lbnRydXN0LmNvbS9DUkxzL0VNU1Jvb3RDQTIuY3JshoGtbGRhcDov
L3Jvb3RkaXIubWFuYWdlZC5lbnRydXN0LmNvbS9jbj1XaW5Db21iaW5lZDIsb3U9
RW50cnVzdCUyME1hbmFnZWQlMjBTZXJ2aWNlcyUyMFJvb3QlMjBDQSxvdT1DZXJ0
aWZpY2F0aW9uJTIwQXV0aG9yaXRpZXMsbz1FbnRydXN0LGM9VVM/Y2VydGlmaWNh
dGVSZXZvY2F0aW9uTGlzdDtiaW5hcnkwgYeggYSggYGkfzB9MQswCQYDVQQGEwJV
UzEQMA4GA1UEChMHRW50cnVzdDEiMCAGA1UECxMZQ2VydGlmaWNhdGlvbiBBdXRo
b3JpdGllczEpMCcGA1UECxMgRW50cnVzdCBNYW5hZ2VkIFNlcnZpY2VzIFJvb3Qg
Q0ExDTALBgNVBAMTBENSTDEwHQYDVR0OBBYEFKlTvmSEg0tdJsYnPi7RhGhVPNB1
MA0GCSqGSIb3DQEBCwUAA4IBAQBEML+28l4774Ljsi9UQVuiJ8rMn3vWxqhSgrWh
OTSKEgHgmqAAz/DSwk9lWSt3MKhXsIYiudW7paB4hIxvPurpOYp1iOTn2JesPOKN
cV865auh+LFr/wBGDYlUMr/X0jnmFVqHHGBn5Ev5OgpWx0x6YDp0PvUFNAzNMNHi
63epqJd9aNwau7oWQqtvW38I1fZzdT/bd3B3zBtJRpbjiJVEeaX6SUXrMT2noMsN
2vBWo++6XpnB7LUPMx5nZQ/EIF1+s7NmX6xjxU8qBOjPLG/lvVf+1bJ1RbmhYXnH
yc374GfU6KTMBfB4hR6pet7+PgFtXubRd0zI7O9gqiwQgZpU
-----END CERTIFICATE-----

[13] Entrust posts all Trusted Root Certificates for Entrust Managed Services (EMS) PKI, at https://federaladminservices.managed.entrust.com/fedcerts/

C.2 Entrust Managed Services SSP CA – Expires 2025

This is the Entrust SSP CA certificate for PIV Cards issued after July 30, 2015 by GSA USAccess.

The following Base-64 blob[14] is for:

Issued to: Entrust Managed Services SSP CA
Issued by: Entrust Managed Services Root CA
Expires: 7/23/2025
Serial Number: 448063d5

To create a ".cer" file, copy everything from and including "-----BEGIN CERTIFICATE-----" thru "-----END CERTIFICATE-----" into a file with an extension ".cer" (e.g. EntrustSSPCA2025.cer).

-----BEGIN CERTIFICATE-----
MIIHQTCCBimgAwIBAgIERIBj1TANBgkqhkiG9w0BAQsFADBuMQswCQYDVQQGEwJV
UzEQMA4GA1UEChMHRW50cnVzdDEiMCAGA1UECxMZQ2VydGlmaWNhdGlvbiBBdXRo
b3JpdGllczEpMCcGA1UECxMgRW50cnVzdCBNYW5hZ2VkIFNlcnZpY2VzIFJvb3Qg
Q0EwHhcNMTUwNzMwMTYzNzQ0WhcNMjUwNzIzMTYzNjM2WjBtMQswCQYDVQQGEwJV
UzEQMA4GA1UEChMHRW50cnVzdDEiMCAGA1UECxMZQ2VydGlmaWNhdGlvbiBBdXRo
b3JpdGllczEoMCYGA1UECxMfRW50cnVzdCBNYW5hZ2VkIFNlcnZpY2VzIFNTUCBD
QTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOAWps85AHSHa7h8Mra/
tS//OaO6Pj4sokxbJc9rYvfzSeevJDw13zwuayYX9eSxJqC7vyevCNr+Et8zm3F2
LJnu66D1e5nVj5HqQtp5fhn3jse1M5aicFuQuZbQNvejxZ+dpzuwmJ/56eRwLcRt
ts6N7vu4+lqhftXM7ItNzeJJ9buOk6G6J2QMRedU5kotAEapPUdZ4f7moc4LYVa0
g2wCa0FCLf24q9gvg4Qm0kYWz1eCYrXuGRbIX2H1I2duF5alv/ebPNB7hkmXdFIy
neJrdBRvt0T+7UmH4Emy/Jda5S22PM1UOtmG9Qbqo9rpOmU4LRomPrPtJPvuY0CP
IQECAwEAAaOCA+YwggPiMA4GA1UdDwEB/wQEAwIBBjCBiAYDVR0gBIGAMH4wDAYK
YIZIAWUDAgEDBjAMBgpghkgBZQMCAQMHMAwGCmCGSAFlAwIBAwgwDAYKYIZIAWUD
AgEDDTAMBgpghkgBZQMCAQMRMAwGCmCGSAFlAwIBAyQwDAYKYIZIAWUDAgEDJzAM
BgpghkgBZQMCAQMoMAwGCmCGSAFlAwIBAykwEgYDVR0TAQH/BAgwBgEB/wIBADCC
AWMGCCsGAQUFBwEBBIIBVTCCAVEwTQYIKwYBBQUHMAKGQWh0dHA6Ly9yb290d2Vi
Lm1hbmFnZWQuZW50cnVzdC5jb20vQUlBL0NlcnRzSXNzdWVkVG9FTVNSb290Q0Eu
cDdjMIG6BggrBgEFBQcwAoaBrWxkYXA6Ly9yb290ZGlyLm1hbmFnZWQuZW50cnVz
dC5jb20vb3U9RW50cnVzdCUyME1hbmFnZWQlMjBTZXJ2aWNlcyUyMFJvb3QlMjBD
QSxvdT1DZXJ0aWZpY2F0aW9uJTIwQXV0aG9yaXRpZXMsbz1FbnRydXN0LGM9VVM/
Y0FDZXJ0aWZpY2F0ZTtiaW5hcnksY3Jvc3NDZXJ0aWZpY2F0ZVBhaXI7YmluYXJ5
MEMGCCsGAQUFBzABhjdodHRwOi8vb2NzcC5tYW5hZ2VkLmVudHJ1c3QuY29tL09D
U1AvRU1TUm9vdENBUmVzcG9uZGVyMIIBiAYDVR0fBIIBfzCCAXsgge6ggeuggeiG
Nmh0dHA6Ly9yb290d2ViLm1hbmFnZWQuZW50cnVzdC5jb20vQ1JMcy9FTVNSb290
Q0EyLmNybIaBrWxkYXA6Ly9yb290ZGlyLm1hbmFnZWQuZW50cnVzdC5jb20vY249
V2luQ29tYmluZWQyLG91PUVudHJ1c3QlMjBNYW5hZ2VkJTIwU2VydmljZXMlMjBS
b290JTIwQ0Esb3U9Q2VydGlmaWNhdGlvbiUyMEF1dGhvcml0aWVzLG89RW50cnVz
dCxjPVVTP2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3Q7YmluYXJ5MIGHoIGEoIGB
pH8wfTELMAkGA1UEBhMCVVMxEDAOBgNVBAoTB0VudHJ1c3QxIjAgBgNVBAsTGUNl
cnRpZmljYXRpb24gQXV0aG9yaXRpZXMxKTAnBgNVBAsTIEVudHJ1c3QgTWFuYWdl
ZCBTZXJ2aWNlcyBSb290IENBMQ0wCwYDVQQDEwRDUkwxMB8GA1UdIwQYMBaAFKlT
vmSEg0tdJsYnPi7RhGhVPNB1MB0GA1UdDgQWBBRVtGwzP+NgGqf/w+209+QE2inQ
YzANBgkqhkiG9w0BAQsFAAOCAQEAHQpB8fe6Cj/DlsRBnP7AKqhR2UFEF+pOFXec
SIP5R3B8cVz9ippRiZrLFdnVfvAjj3xEQAxqTJlLNVjcNGtHuvklhmebsXlCEoHm
grRYuAoAyhu92IyQ1+cq77mOlpVbmE6AsXsUvh9zBTlavsXJ0RhfQ49JJD6nPuda
rO8Dl6ehTFpxpzEqhieGso4XDu3tLl3Z6kOe2Hgfp9CdEf7rRjJPdLpv/RFGPbsx
YJ7V4c1ryxnbCP0IDF8zw0Ocuw08tvtP4YdSid+FcR7PoGqKXBUdOJR6GwIP6n3F
FVgoq2/4mMrZ1ZDmz2mbS/O6xdllRc99aHA9MHvbq/EpE5dr3g==
-----END CERTIFICATE-----

[14] Entrust posts all Trusted Root Certificates for Entrust Managed Services (EMS) PKI, at https://federaladminservices.managed.entrust.com/fedcerts/

C.3 Entrust Managed Services Root CA – Expires 2019

This is the Entrust Root CA certificate for PIV Cards issued prior to July 30, 2015 by GSA USAccess.

The following Base-64 blob[15] is for:

Issued to: Entrust Managed Services Root CA
Issued by: Entrust Managed Services Root CA
Expires: 5/9/2019
Serial Number: 447f9cf2

To create a ".cer" file, copy everything from and including "-----BEGIN CERTIFICATE-----" thru "-----END CERTIFICATE-----" into a file with an extension ".cer" (e.g. EntrustRoot2019.cer).

-----BEGIN CERTIFICATE-----
MIIGUDCCBTigAwIBAgIERH+c8jANBgkqhkiG9w0BAQUFADBuMQswCQYDVQQGEwJV
UzEQMA4GA1UEChMHRW50cnVzdDEiMCAGA1UECxMZQ2VydGlmaWNhdGlvbiBBdXRo
b3JpdGllczEpMCcGA1UECxMgRW50cnVzdCBNYW5hZ2VkIFNlcnZpY2VzIFJvb3Qg
Q0EwHhcNMDkwNTA5MTMzMjMxWhcNMTkwNTA5MTQwMjMxWjBuMQswCQYDVQQGEwJV
UzEQMA4GA1UEChMHRW50cnVzdDEiMCAGA1UECxMZQ2VydGlmaWNhdGlvbiBBdXRo
b3JpdGllczEpMCcGA1UECxMgRW50cnVzdCBNYW5hZ2VkIFNlcnZpY2VzIFJvb3Qg
Q0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC2e3PT/tEkZVdlrqJK
qzlovKz4I0EGnD/47mhE5DutIji2fPZY/GKo9oLV10C8pFZxvb5pS9gwl9GR2myz
3EEfqdFnmX+XCRDN+BOw5C0qUW/6tPYpV1QVdGKSn8IBQORXKILuI++LyQeA0rhp
iBRt8bDGbCtLvuf1ywHc2/lrWOOkwlAzwJd15D6dnbBS2IwgwwclFXCtOf/bn051
p8uP/8Y7+smiUAzsTg82bQ7ph3HTqHMeTLEGPeNBrV3Ct3EXO8iTCh1UD3JVf+LQ
VWzy96iYxm4WIE+xL54fiLEAKvi3+RCTaWUDpylYKGsqu7y9c0d8n/g780SItWUo
gLulAgMBAAGjggL0MIIC8DCCASAGCCsGAQUFBwELBIIBEjCCAQ4wgboGCCsGAQUF
BzAFhoGtbGRhcDovL3Jvb3RkaXlubWFuYWdlZC5lbnRydXN0LmNvbS9vdT1FbnRy
dXN0JTIwTWFuYWdlZCUyMFNlcnZpY2VzJTIwUm9vdCUyMENBLG91PUNlcnRpZmlj
YXRpb24lMjBBdXRob3JpdGllcyxvPUVudHJ1c3QsYz1VUz9jQUNlcnRpZmljYXRl
O2JpbmFyeSxjcm9zc0NlcnRpZmljYXRlUGFpcjtiaW5hcnkwTwYIKwYBBQUHMAWG
Q2h0dHA6Ly9yb290d2ViLm1hbmFnZWQuZW50cnVzdC5jb20vU0lBL0NBY2VydHNJ
c3N1ZWRCeUVNU1Jvb3RDQS5wN2MwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E
BAMCAQYwggGIBgNVHR8EggF/MIIBezCB7qCB66CB6IaBrWxkYXA6Ly9yb290ZGly
Lm1hbmFnZWQuZW50cnVzdC5jb20vY249V2luQ29tYmluZWQxLG91PUVudHJ1c3Ql
MjBNYW5hZ2VkJTIwU2VydmljZXMlMjBSb290JTIwQ0Esb3U9Q2VydGlmaWNhdGlv
biUyMEF1dGhvcml0aWVzLG89RW50cnVzdCxjPVVTP2NlcnRpZmljYXRlUmV2b2Nh
dGlvbkxpc3Q7YmluYXJ5hjZodHRwOi8vcm9vdHdlYi5tYW5hZ2VkLmVudHJ1c3Qu
Y29tL0NSTHMvRU1TUm9vdENBMS5jcmwwgYeggYSggYGkfzB9MQswCQYDVQQGEwJV
UzEQMA4GA1UEChMHRW50cnVzdDEiMCAGA1UECxMZQ2VydGlmaWNhdGlvbiBBdXRo
b3JpdGllczEpMCcGA1UECxMgRW50cnVzdCBNYW5hZ2VkIFNlcnZpY2VzIFJvb3Qg
Q0ExDTALBgNVBAMTBENSTDEwHQYDVR0OBBYEFJxiZiadcbandVNk4ayxxyU8RF0N
MA0GCSqGSIb3DQEBBQUAA4IBAQBpmyez/kdiPz0HPCnUPaEMf2o2Lfzu/fO5CCX9
jxN12sHTHD/hxnkTTS6aetDxL6Q0WvWSHBdkT0VfqNegaZ0rD+YX2YbEFpQaPraV
bk/GUFGWzvHZIP26msVBWs7y8GdWPOOLVvdVOzgRTBFzE8zPS85imkPbkVe5eRc3
XTowNUurA0ldxbvCZi8XGN5Lw0Ge0J8106qV2uHsVvutZ4Rk2+l6Bb2q6QRo+/Pv
m96V5OLvMBC6FnjTsXZ+r4ry2cQsl5i9MdT/du2mnV2IMTpm990NABrEj4lVDKuy
7QwQ/CWARykKoFpLgD2nIKnTxIXssnFfn4y0rW5i66hWZwUp
-----END CERTIFICATE-----

[15] Entrust posts all Trusted Root Certificates for Entrust Managed Services (EMS) PKI, at https://federaladminservices.managed.entrust.com/fedcerts/

C.4 Entrust Managed Services SSP CA – Expires 2019

This is the Entrust SSP CA certificate for PIV Cards issued prior to July 30, 2015 by GSA USAccess.

The following Base-64 blob[16] is for:

Issued to: Entrust Managed Services SSP CA
Issued by: Entrust Managed Services Root CA
Expires: 5/9/2019
Serial Number: 447f9d1f

To create a ".cer" file, copy everything from and including "-----BEGIN CERTIFICATE-----" thru "-----END CERTIFICATE-----" into a file with an extension ".cer" (e.g. EntrustSSPCA2019.cer).

-----BEGIN CERTIFICATE-----
MIIHBDCCBeygAwIBAgIERH+dHzANBgkqhkiG9w0BAQUFADBuMQswCQYDVQQGEwJV
UzEQMA4GA1UEChMHRW50cnVzdDEiMCAGA1UECxMZQ2VydGlmaWNhdGlvbiBBdXRo
b3JpdGllczEpMCcGA1UECxMgRW50cnVzdCBNYW5hZ2VkIFNlcnZpY2VzIFJvb3Qg
Q0EwHhcNMDkwNTA5MTUzMjA2WhcNMTkwNTA5MTQwMjMxWjBtMQswCQYDVQQGEwJV
UzEQMA4GA1UEChMHRW50cnVzdDEiMCAGA1UECxMZQ2VydGlmaWNhdGlvbiBBdXRo
b3JpdGllczEoMCYGA1UECxMfRW50cnVzdCBNYW5hZ2VkIFNlcnZpY2VzIFNTUCBD
QTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAL4Y6xZWI7Bkvhi+89Hw
IW5REGezeZthIq5dJoUYkrwDlbFBXZTxn9E4PnPEmZcznpNE5ru20jXFRBzsFOlk
NKCFH1NborQoC8WDnc42qCNzHXRBS0mJYxivkRH6abt1m7QvpVXNOrtLgVAAwyu7
48m+IBP7uPUlHqGyAV0ePih/z+AeYmuZYxZtAoev6HKohyW2e9ZR2bXqWp6tcM0H
F+czsWGAVPZ1h3hVU+CNCvudPTYCnI2BrT7t6b1pYG5jc8UO1dnABKvNPvERNgi4
HSoTMMhzvHFVT9WXDp4endEoXjc0pzsEjV4J0pJz11Sck0TQ+IAroDw3PzfTGOgz
g10CAwEAAaOCA6kwggOlMA4GA1UdDwEB/wQEAwIBBjBPBgNVHSAESDBGMAwGCmCG
SAFlAwIBAwYwDAYKYIZIAWUDAgEDBzAMBgpghkgBZQMCAQMIMAwGCmCGSAFlAwIB
Aw0wDAYKYIZIAWUDAgEDETAPBgNVHRMBAf8EBTADAQH/MIIBYwYIKwYBBQUHAQEE
ggFVMIIBUTCBugYIKwYBBQUHMAKGga1sZGFwOi8vcm9vdGRpci5tYW5hZ2VkLmVu
dHJ1c3QuY29tL291PUVudHJ1c3QlMjBNYW5hZ2VkJTIwU2VydmljZXMlMjBSb290
JTIwQ0Esb3U9Q2VydGlmaWNhdGlvbiUyMEF1dGhvcml0aWVzLG89RW50cnVzdCxj
PVVTP2NBQ2VydGlmaWNhdGU7YmluYXJ5LGNyb3NzQ2VydGlmaWNhdGVQYWlyO2Jp
bmFyeTBNBggrBgEFBQcwAoZBaHR0cDovL3Jvb3R3ZWIubWFuYWdlZC5lbnRydXN0
LmNvbS9TSUEvQ2VydHNJc3N1ZWRUb0VNU1Jvb3RDQS5wN2MwQwYIKwYBBQUHMAGG
N2h0dHA6Ly9vY3NwLm1hbmFnZWQuZW50cnVzdC5jb20vT0NTUC9FTVNSb290Q0FS
ZXNwb25kZXIwggGIBgNVHR8EggF/MIIBezCB7qCB66CB6IaBrWxkYXA6Ly9yb290
ZGlyLm1hbmFnZWQuZW50cnVzdC5jb20vY249V2luQ29tYmluZWQxLG91PUVudHJ1
c3QlMjBNYW5hZ2VkJTIwU2VydmljZXMlMjBSb290JTIwQ0Esb3U9Q2VydGlmaWNh
dGlvbiUyMEF1dGhvcml0aWVzLG89RW50cnVzdCxjPVVTP2NlcnRpZmljYXRlUmV2
b2NhdGlvbkxpc3Q7YmluYXJ5hjZodHRwOi8vcm9vdHdlYi5tYW5hZ2VkLmVudHJ1
c3QuY29tL0NSTHMvRU1TUm9vdENBMS5jcmwwgYeggYSggYGkfzB9MQswCQYDVQQG
EwJVUzEQMA4GA1UEChMHRW50cnVzdDEiMCAGA1UECxMZQ2VydGlmaWNhdGlvbiBB
dXRob3JpdGllczEpMCcGA1UECxMgRW50cnVzdCBNYW5hZ2VkIFNlcnZpY2VzIFJv
b3QgQ0ExDTALBgNVBAMTBENSTDEwHwYDVR0jBBgwFoAUnGJmJp1xtqd1U2ThrLHH
JTxEXQ0wHQYDVR0OBBYEFNPO51uJp81skcZnNqlYcgns4jnzMA0GCSqGSIb3DQEB
BQUAA4IBAQB1efbjA0HgDMfS7KKmEWnOC5SzYg68tipgd0NXEpsjXLYlJny2JJ0R
OZfTWfQwvnYKBitapDFD8SlxJVd5dNnyo+tYhsQec3u6PfgQlBM8lTaJtmKbV1Rf
0Iqg+LCFMGno04hf2y6nhKMiDmuRk2BZmP6CBF5Z+2hY1VKcEllTk5klXJcpRZIA
MaYAILfC+4w7lYy3E+g7QODA0TSYp0AT/uDZwRrDFbUj2Hzpe/DlrQd1QbU9gOpM
z4+XV1BIghkJ9o8n5IL4htk8i1rfaN0JFEiz/FKSsnpPpFmL+7z5QPR3NAumcSfk
ae8ZK+tNTIAIXf1W3wFfUpcNigYJlKgj
-----END CERTIFICATE-----

[16] Entrust posts all Trusted Root Certificates for Entrust Managed Services (EMS) PKI, at https://federaladminservices.managed.entrust.com/fedcerts/

Appendix D Exporting PIV Authentication Certificate from PIV Card

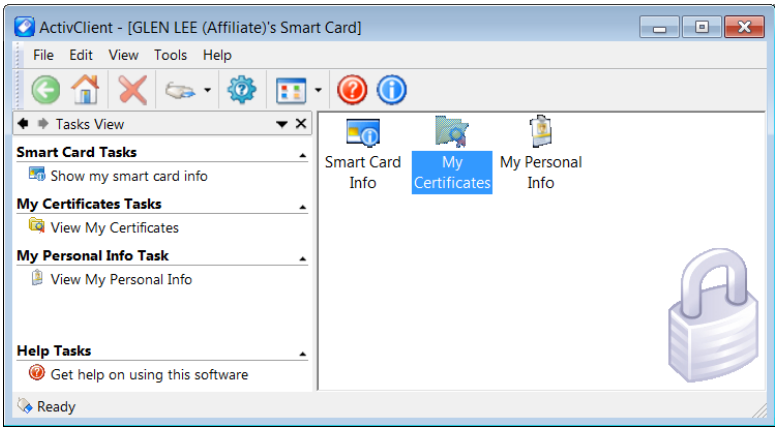
The *PIV Authentication Certificate* can be exported from the PIV Card into a certificate (.cer) file. Only the public key certificate is exported in this process. The PIV Card restricts the ability to export private keys.

- See D.1 for computers with ActivIdentity ActivClient installed
- See D.2 for computers without ActivIdentity ActivClient installed

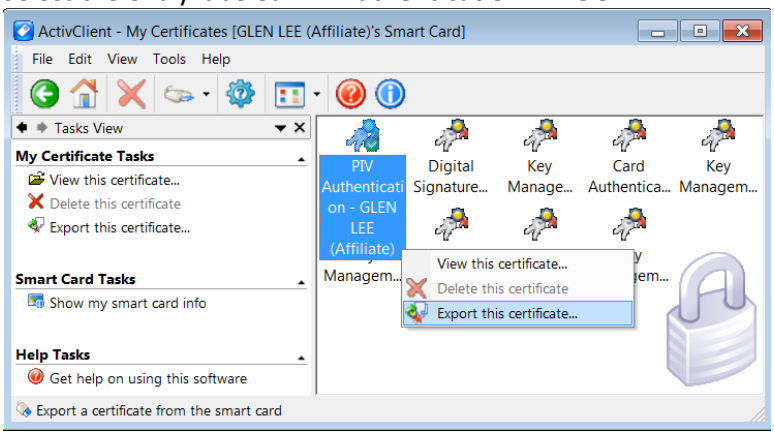
D.1 Exporting PIV Authentication Certificate using ActivIdentity ActivClient

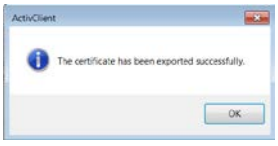
To export to a certificate (.cer) file:

1. *Insert* **PIV Card** into the smart card reader.
2. *Launch* **ActivClient User Console** by *clicking* **Start | All Programs | ActivIdentity | ActivClient | User Console**



3. *Double-click* on **My Certificates** icon located in the right pane
4. *Select* the entry labeled **PIV Authentication - <YOUR NAME>**



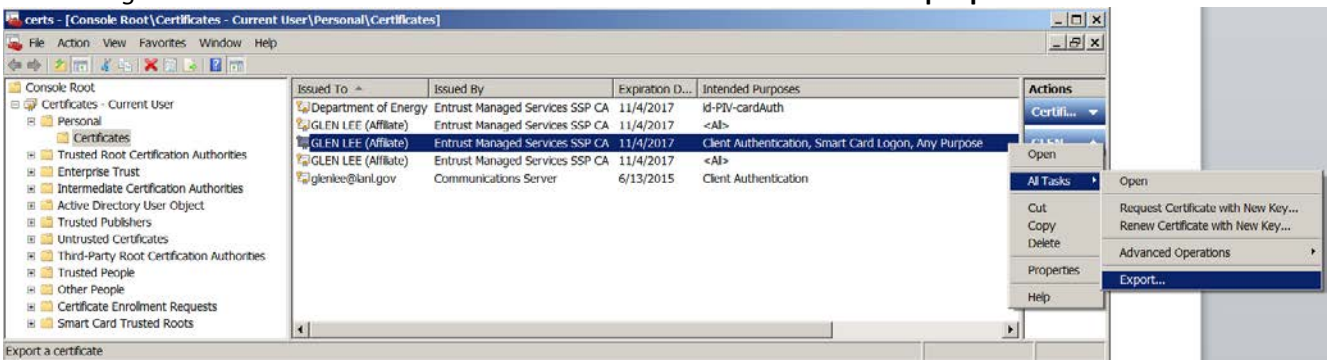
5. *Right-click* on the entry *Select* **"Export this certificate"**
6. *Type* the name of the file and *save* it to a location on the computer
7. When completed, you should see 

and the certificate (.cer) file created in the location you selected during the export process.

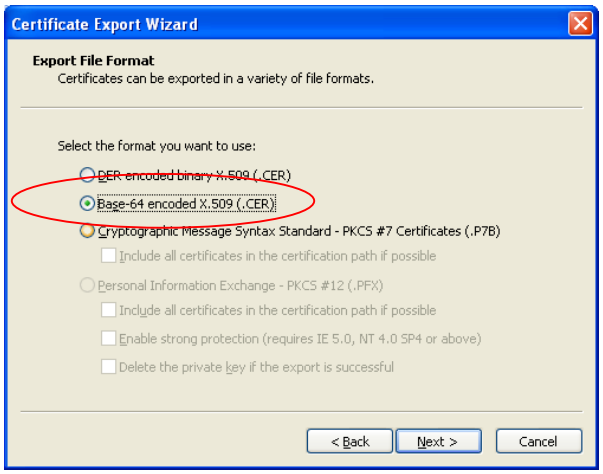
D.2 Exporting PIV Authentication Certificate using native Microsoft tools

To export to a certificate (.cer) file:

1. *Insert* **PIV Card** into the smart card reader.
2. *Launch* MMC Console by *clicking* **Start** and *typing* **MMC** in the **"*Search programs and files*"** text box
3. *Click* **File | Add / Remove Snap-in**
4. *Select* **"Certificates"** then *click* **Add** button
5. *Click* **OK**
6. *Navigate* to **Certificates – Current User | Personal | Certificates**
7. *Select* the **PIV Authentication Certificate** that is on the PIV card.
    a. It is the one that says "Client Authentication, Smart Card Logon" in the **Certificate Intended Purposes** column.
8. *Right-click* on the **PIV Authentication Certificate** and *select* **All Tasks | Export**



9. *Follow* the instructions of the **Certificate Export Wizard**.
    a. When prompted for "Export File Format", *select* **"Base-64 encoded X.509 (.CER)"**. This will allow the file to be read by a text editor as well.



10. When completed, you should see 

and the certificate (.cer) file created in the location you selected during the export process.

Appendix E CRL and OCSP Sources

#	Type	Validates	Original Source	DOE HQ Source	Notes
1.	CRL	DOE PIV Cards	http://sspweb.managed.entrust.com/CRLs/EMSSSPCA2.crl	http://pki.energy.gov/crls/entrust/EMSSSPCA2.crl	CRL that validates PIV Cards issued after July 30, 2015. Also validates other Agencies' PIV Cards that use Entrust Managed Service SSP.
2.	CRL	DOE PIV Cards	http://rootweb.managed.entrust.com/CRLs/EMSRootCA2.crl	http://pki.energy.gov/crls/entrust/EMSRootCA2.crl	CRL that validates all CAs issued from Entrust Managed Services Root after July 30, 2015.
3.	CRL	DOE PIV Cards	http://sspweb.managed.entrust.com/CRLs/EMSSSPCA1.crl	http://pki.energy.gov/crls/entrust/EMSSSPCA1.crl	SHA 2 version of CRL that validates PIV Cards issued prior to July 30, 2015. Also validates other Agencies' PIV Cards that use Entrust Managed Service SSP.
4.	CRL	DOE PIV Cards	http://sspweb.managed.entrust.com/CRLs/EMSSSPCA.crl	http://pki.energy.gov/crls/entrust/EMSSSPCA.crl	SHA 1 version of CRL that validates PIV Cards issued prior to July 30, 2015. Also validates other Agencies' PIV Cards that use Entrust Managed Service SSP.
5.	CRL	DOE PIV Cards	http://rootweb.managed.entrust.com/CRLs/EMSRootCA1.crl	http://pki.energy.gov/crls/entrust/EMSRootCA1.crl	SHA 2 version of CRL that validates all CAs issued from Entrust Managed Services Root prior to July 30, 2015.
6.	CRL	DOE PIV Cards	http://rootweb.managed.entrust.com/CRLs/EMSRootCA.crl	http://pki.energy.gov/crls/entrust/EMSRootCA.crl	SHA 1 version of CRL that validates all CAs issued from Entrust Managed Services Root prior to July 30, 2015.
7.	OCSP	DOE PIV Cards	http://ocsp.managed.entrust.com/OCSP/EMSSSPCAResponder	http://pki.energy.gov	Also validates other Agencies' PIV Cards that use Entrust Managed Service SSP.
8.	OCSP	DOE PIV Cards	http://ocsp.managed.entrust.com/OCSP/EMSRootCAResponder	http://pki.energy.gov	Validates all CAs issued from Entrust Managed Services Root.

Appendix F Axway Desktop Validator Enterprise Configurations

Several configurations were developed to support revocation status checking on the Windows AD DCs.

- A standard configuration, called *"Standard Configuration",*
- Several contingency options that can be deployed to support business continuity should issues occur that are associated with revocation status checking.

In this Appendix:

F.1 DVE Configuration Files

Several configurations were developed to support revocation status checking on the Windows AD DCs:

- A standard configuration, called *"Standard Configuration",*
- Several contingency options that can be deployed to support business continuity should issues occur that are associated with revocation status checking. Appendix F.7 provides guidance on when to apply the various contingency options.

These configurations are documented in this Appendix F. Table 4 identifies each configuration and a recommended location for the configuration files (both manual import files and Group Policy files) so they are accessible by all DCs.

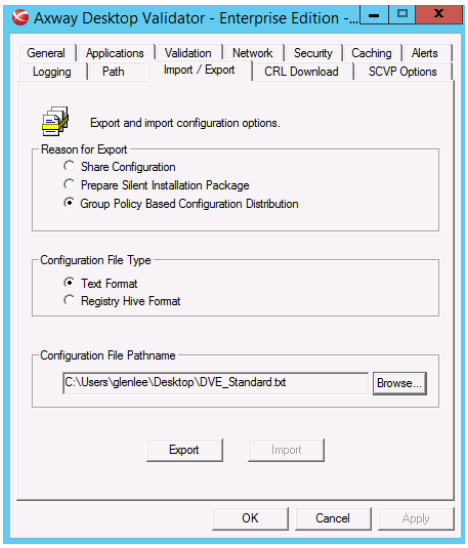
Table 4: DVE Configurations

DVE Standard Configuration (Documented in Appendix F.3)		
	Manual Import	*[domain]*\NETLOGON\DVE\Manual*DVE Standard Configuration.txt*
	Group Policy	*[domain]*\NETLOGON\DVE\GP*DVE_Standard.txt*
DVE Contingency Option 1 (Documented in Appendix F.4)		
	Manual Import	*[domain]*\NETLOGON\DVE\Manual*DVE Contingency Option 1.txt*
	Group Policy	*[domain]*\NETLOGON\DVE\GP*DVE_CO1.txt*
DVE Contingency Option 2 (Documented in Appendix F.5)		
	Manual Import	*[domain]*\NETLOGON\DVE\Manual*DVE Contingency Option 2.txt*
	Group Policy	*[domain]*\NETLOGON\DVE\GP*DVE_CO2.txt*
DVE Contingency Option 3 (Documented in Appendix F.6)		
	Manual Import	*[domain]*\NETLOGON\DVE\Manual*DVE Contingency Option 3.txt*
	Group Policy	*[domain]*\NETLOGON\DVE\GP*DVE_CO3.txt*

These were created using DVE's *Import / Export tab*, which provides options of generating configuration files in the proper formats for manual importing or using Group Policy to apply configuration changes to the DVE.

DVE Configuration Files can be generated by:

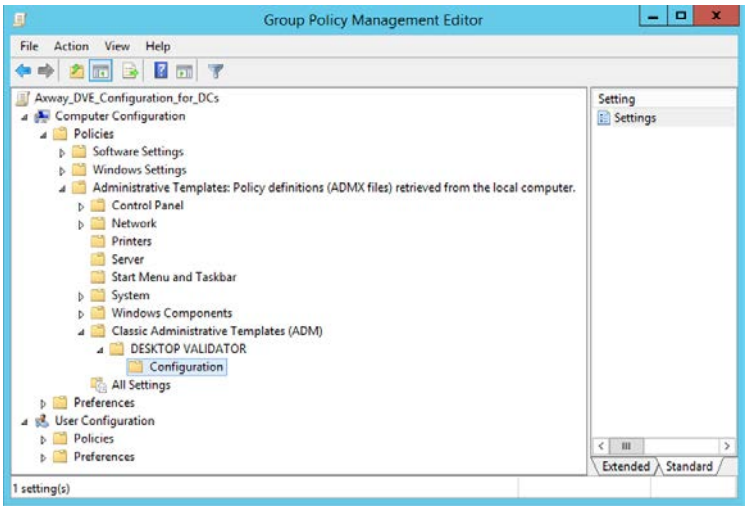
1. Configuring one instance of DVE with all the desired settings
2. Generating the Group Policy configuration file by:
   a. *Selecting* the **DVE Import / Export** tab
   b. *Selecting* **"Group Policy Based Configuration Distribution"** option under **"Reason for Export"**
   c. *Browsing* to a file location (e.g., Desktop) and *typing* an appropriate file name
   d. *Clicking* **Export** button



F.2 DVE Group Policy Object

A Group Policy Object (GPO) called, *Axway_DVE_Configuration_for_DCs*, should be established using the using Group Policy Management tool.

1. *Launch* **Group Policy Management** tool
2. *Create* the GPO called, ***Axway_DVE_Configuration_for_DCs***
3. *Add* the **Axway DVE administrative template (ADMX)**:
   a. *Copied* **dv.*admx*[17]** to *%systemroot%***\policyDefinitions**
   b. *Copied* **dv.adml[18]** to *%systemroot%***\policyDefinitions\en-us**
   c. *Launched* **Group Policy Management Editor** to confirm template was added by navigating to: **Computer Configuration | Policies | Administrative Templates | DESKTOP VALIDATOR | Configuration**
4. *Link* GPO to **Domain Controllers**
5. *Apply* GPO to **Authenticated Users**, which will apply GPO to all DCs



[17] dv.admx file is located at **C:\Program Files\Tumbleweed\Desktop Validator**

[18] dv.admxl file is located at **C:\Program Files\Tumbleweed\Desktop Validator\en-US**

F.3 Standard Configuration

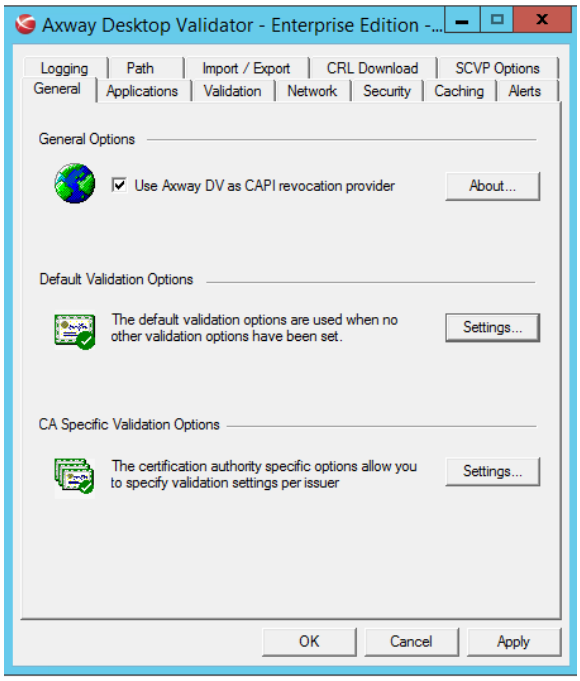
This section specifies the specific DVE configurations for the standard operational usage in deployment. Included in the details is rationale (if appropriate) for the configuration as well as observations or lessons learned when testing the configuration.

F.3.1 General (tab)

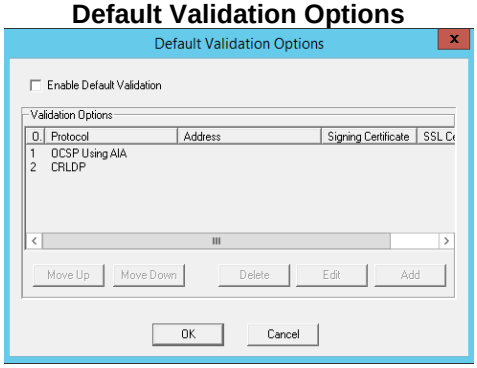
The General tab configures DVE settings that dictates

1. If DVE perform the validation of PKI certificates, instead of using native Microsoft CAPI (see General Options).
   If unchecked, the native Microsoft CAPI will perform all the revocation status checking and all configurations in DVE will be ignored
2. How DVE validates PKI certificates issued by CAs that have not been specifically configured in the DVE (see Default Validation Options)
   As shown in **Default Validation Options**, the "Default Validation" is disabled. The DCs are only going to validate certificates from "known" (or "expected") CAs, which are configured in the *CA Specific Validation Options*

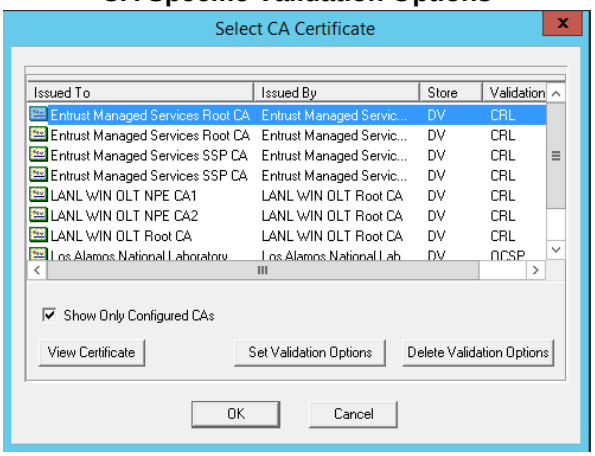
General Tab



Default Validation Options



CA Specific Validation Options



3. Configurations on how PKI certificates from the CA should be validated (e.g., CRL, OCSP) as well as other settings (see CA Specific Validation Options)
   As shown in **CA Specific Validation Options**, the CAs that DVE recognizes as eligible PKI certificate issuers that need to be validated (i.e., perform a revocation status check):
   - The Entrust Root CA and the Entrust SSP CA are the CAs in the certificate chain of the PIV Authentication Certificate on DOE PIV Cards. There are two sets:
     - Root and SSP (expiring in 2019) for PIV Cards issued prior to July 30, 2015
     - Root and SSP (expiring in 2025) for PIV Cards issued post July 30, 2015
   - The OLT PKI CAs (Root and Issuing CAs) that issue PKI certificates to the Domain Controllers

The following sections describe the "Validation Options" (i.e., "Set Validation Options" button) for the CAs.

Entrust CAs

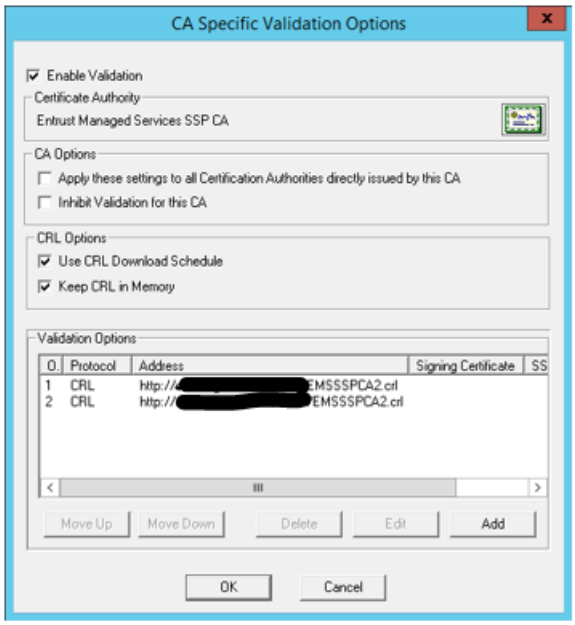
There are two sets of Entrust CAs that are configured

1) Entrust CAs that expire in 2025 and are required for DOE PIV Cards issued after July 30, 2015.
2) Entrust CAs that expire in 2019 and are required for DOE PIV Cards issued prior to July 30, 2015.

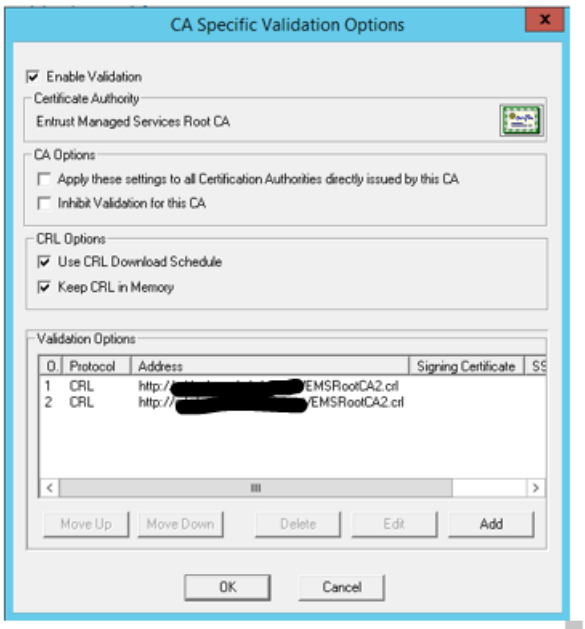
The following are the configurations applied to each CA:

- The DVE is configured to use CRLs to validate certificates, which is more efficient when validating thousands of logons with PKI certificates from the same issuing CA.
- The CRLs are retrieved from Local CRL Repository, which has two URLs for failover purposes.
- The CRLs are pre-fetched on download schedule as configured in the *CRL Download* tab (See Section F.3.8)
- The CRLs are also kept in memory after DVE uses the first time in order to improve performance

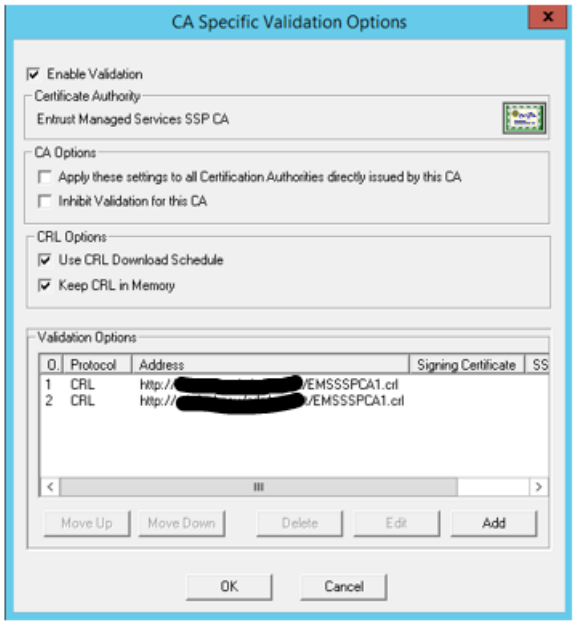
Entrust SSP CA (expires 2025)



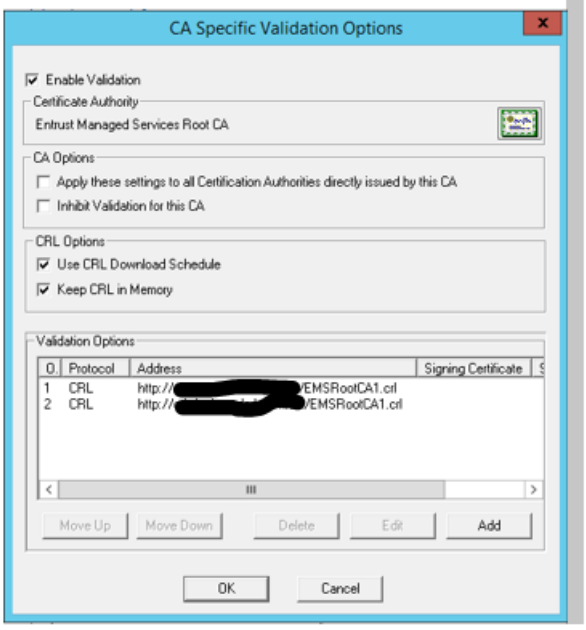
Entrust Root CA (expires 2025)



Entrust SSP CA (expires 2019)



Entrust Root CA (expires 2019)

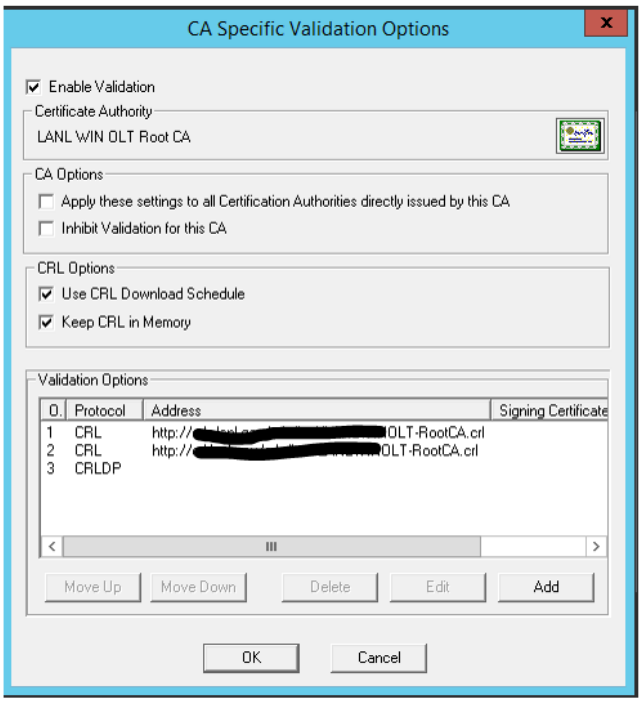


OLT PKI

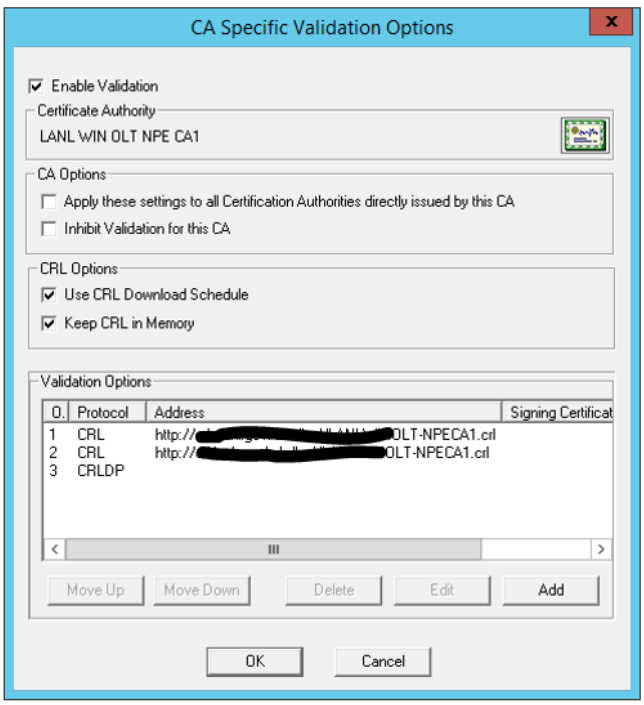
The following are the configurations applied to each CA in the OLT PKI:

- The DVE is configured to use CRLs to validate certificates, which is more efficient when validating thousands of logons with PKI certificates from the same issuing CA.
- The CRLs are retrieved from Local CRL Repository and via CRL Distribution Point (CRLDP) encoded in the certificate as a fallback
- The CRLs are pre-fetched on download schedule as configured in the *CRL Download* tab (See Section F.3.8)
- The CRLs are also kept in memory after DVE uses the first time in order to improve performance

OLT Root CA



OLT NPE CA1

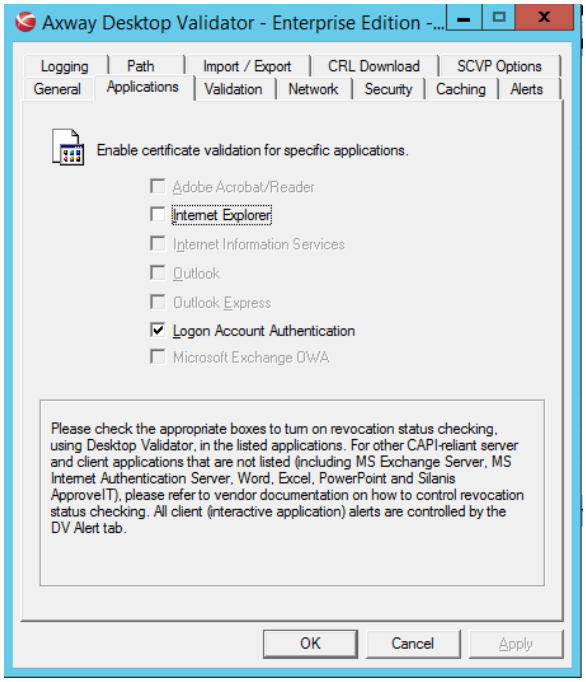


F.3.2 Applications (tab)

The **Applications Tab** shows all current applications on the computer/server on which the DVE is installed and might require a certification revocation status check.

- On the DCs, the only applications relevant to validating certificates are *Internet Explorer* and *Logon Account Authentication* (i.e., PIV logon).
- Since browsing external sites shouldn't be done from DCs, there's no need to have *Internet Explorer* selected, though it can be.
- At a minimum, *Logon Account Authentication* must be checked, which is proposed as the standard configuration for normal operations.

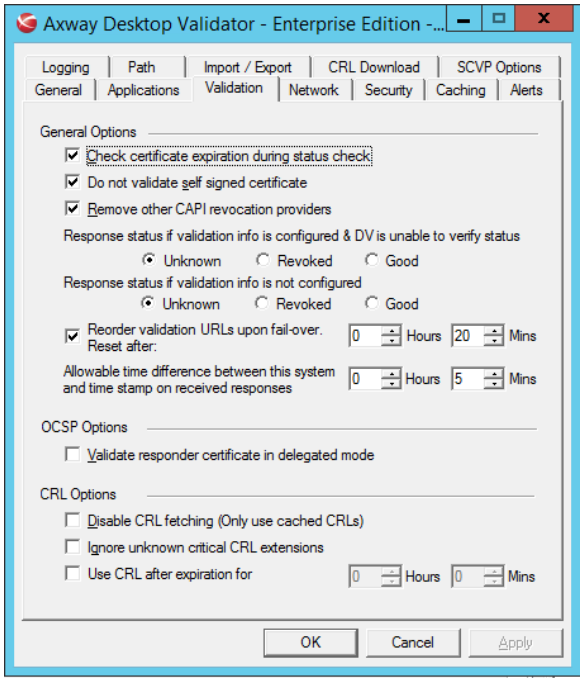
Applications Tab



F.3.3 Validation (tab)

With the exception of one of the *General Options*, the configurations in **Validation Tab** are the default configurations upon installing the DVE. These are the recommended settings when using CRLS and/or OCSP data from the sources configured in *CA-Specific Validation Options* of the *General tab* (see Section F.3.1).

Validation tab



The additional *General Option* configuration is:

- *Reorder validation URLs upon fail-over. Reset after: 20 Mins*

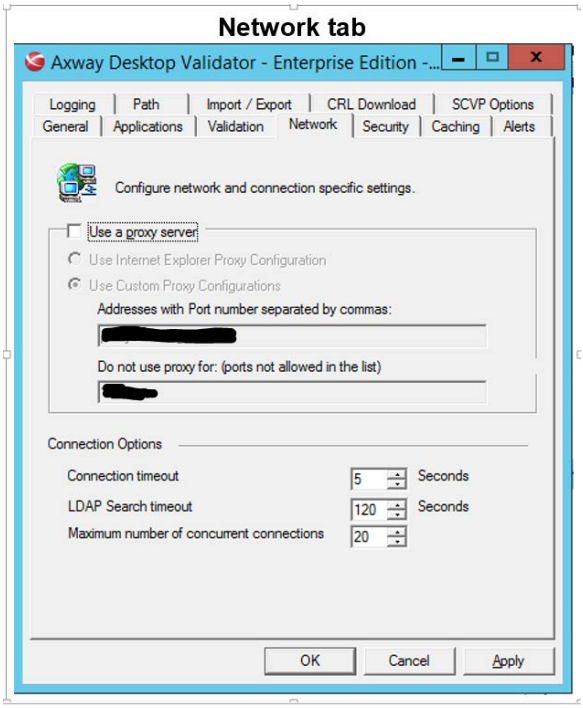
For any CA in the *CA-specific Validation Options* that has multiple configurations, this setting allows DVE to reorder and avoid continuing to use an option that fails repeatedly. If one option continues to fail, it will be temporarily moved to the bottom. This prevents the audit log from being populated with unnecessary errors.

The remaining configuration options in this tab allow us to develop fault tolerant and contingency configurations to apply at times when fresh revocation data is not available. The Contingency Options are addressed in a separate section.

F.3.4 Network (tab)

The **Network tab** is where a proxy server would be configured if the DCs needed to access entities for revocation data that are external to the network. Since the DCs are not permitted outbound access and the LCR is being leveraged for all CRL information, there is no need to have the network proxy configured.

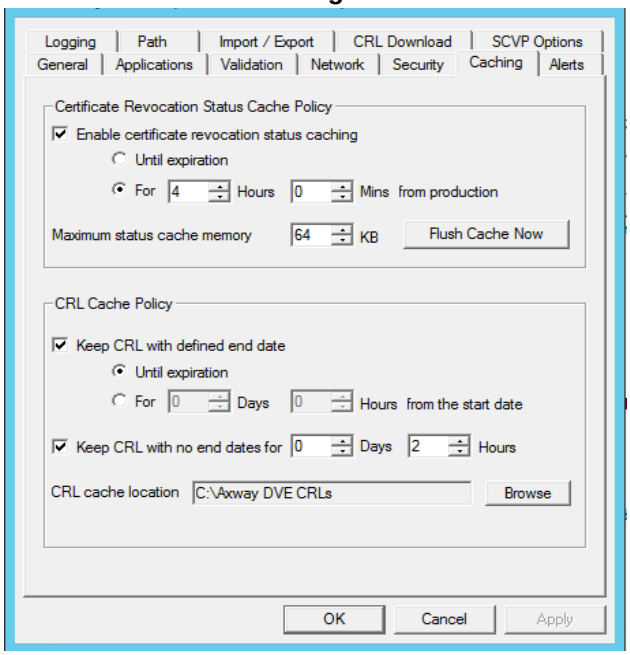
Network tab



F.3.5 Caching (tab)

The **Caching tab** shows the configuration for how DVE caches results of revocation status checks (top portion) and where to download and store CRLs (bottom portion).

Caching tab

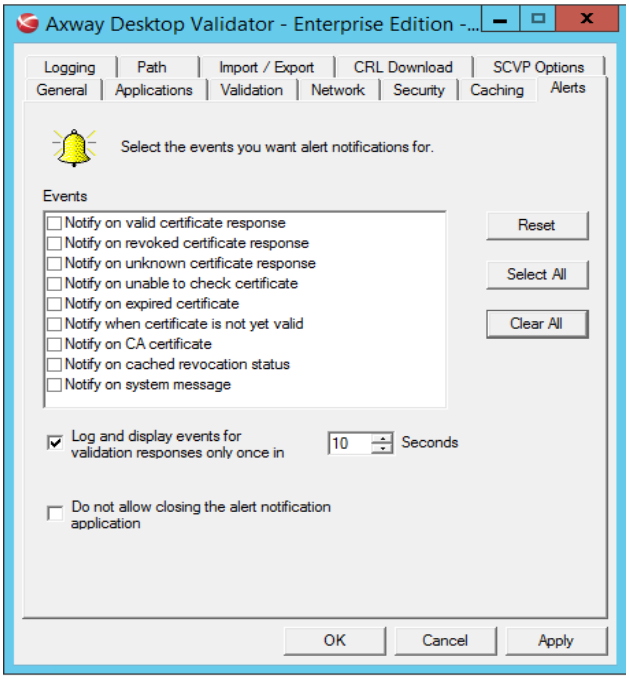


- *Certificate Revocation Status Cache Policy*
  - Caching time is set for 4 hours, which means that DVE will retain and use the result of a status check for up to 4 hours prior to generating a new revocation status check against a CRL or OCSP service.
  - By caching for a period of time, the DVE doesn't have to seek and generate a new result for processes that make multiple requests, which would cause significant latency and performance issues that would impact the user during logon.
  - This aligns with the CRL Download schedule that is polling for new CRLs every 4 hours (See Section F.3.8). The status responses will not be valid longer than the CRL.
- *CRL Cache Policy*
  - All default configurations remain upon installation of DVE, with the exception of the *CRL cache location*
    - The CRL directory was created at the root so that it is easy to locate all CRLs that DVE consumes.
    - When configuring the CRL Download tab (See Section F.3.8), this is the location that the downloaded CRLs are stored.

F.3.6 Alerts (tab)

The "alerts" are pop-up notifications in the system tray, which is unnecessary for DCs. Therefore, all of them have been cleared in the **Alerts Tab**. This does not impact events posted to the Event Viewer application log called, Tumbleweed.

Alerts tab



The item that needs to remain configured is "*Log and display events for validation responses only once in x Seconds"*.

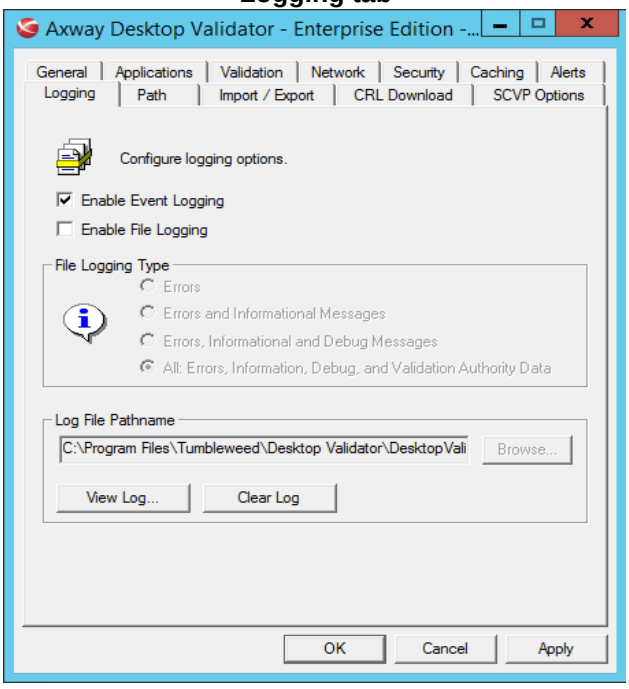
- By specifying a duration greater than 0, this prevents DVE from reporting multiple events for the same certificate being validated.
- As stated in Section F.3.5, multiple validation requests take place for a single validation. The event log would be filled with redundant messages unless this configuration is made.

F.3.7 Logging (tab)

The **Logging tab** gives 3 options for capturing audit events:

1. Via the *Event Viewer*
2. Via a log file
3. Both *Event Viewer* and log file

Logging tab



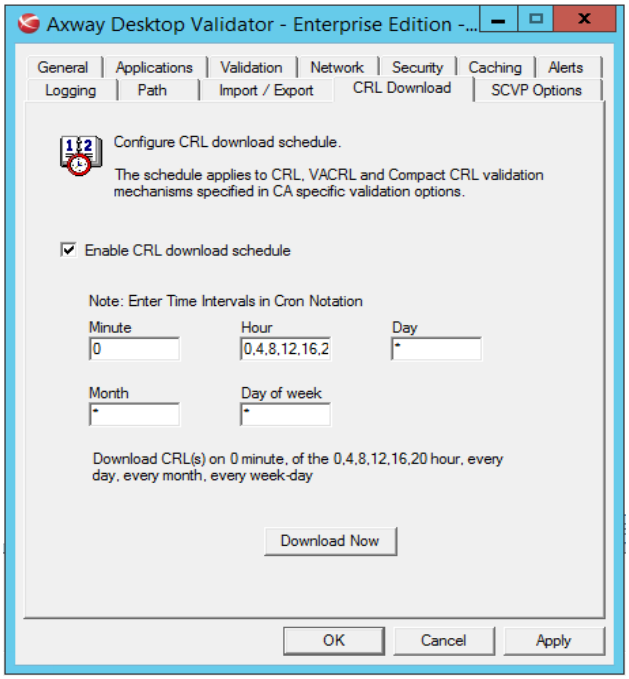
For normal operational usage, the Event Viewer should be used exclusively.

- *"Enable File Logging"* is useful for troubleshooting scenarios only. These the file logs can get significantly large, especially for DCs that are authenticating thousands of users a day.

F.3.8 CRL Download (tab)

For CRLs that are specified in the *CA Specific Validation Options* identified in Section F.3.1, the **CRL Download tab** provides the ability to schedule the time and frequency of the downloads. This is ideal so that DVE doesn't have to fetch a CRL at the time of a status check, which could cause latency and slowness to the authentication process.

CRL Download tab



The standard configuration:

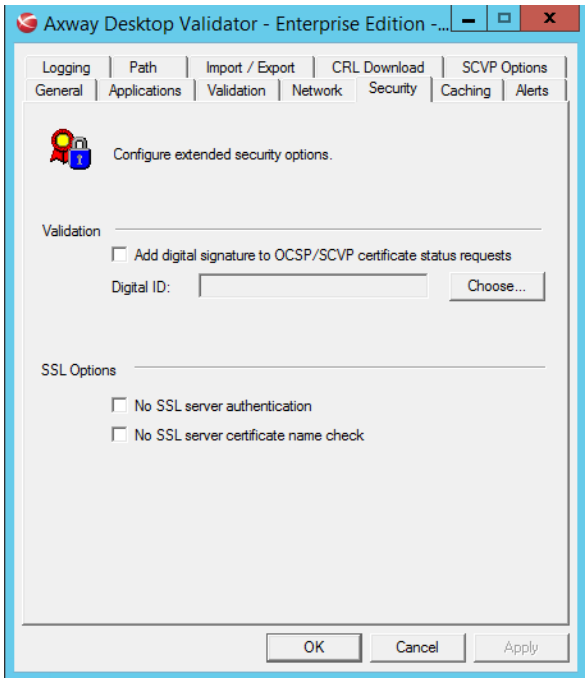
- Fetches CRLs every 4 hours on a daily basis to the location specified on the **Caching tab** in Section F.3.5.
- Fetches CRLs if the CRL at the source location is newer than the CRL already stored in location specified on the **Caching tab** in Section F.3.5.
- Fetches CRLs from only those locations that are configured in the *CA Specific Validation Options* (See Section F.3.1)

This strategy increases the likelihood of detecting a revoked PIV certificate sooner than if we were using traditional CRL checking where CRLs are only fetched when they are set to expire (up to 48 hours for PIV).

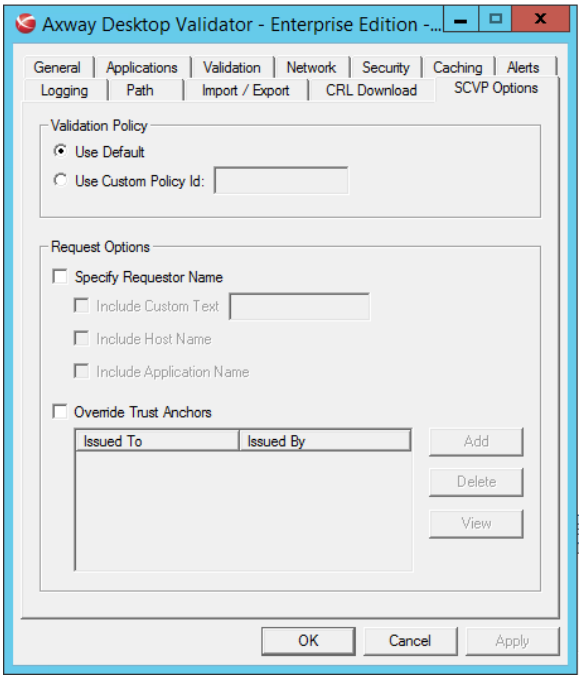
F.3.9 Other tabs

After vendor documentation review and assessing the functionality, the following tabs do not require modifications from the installation defaults. The figures show how the DVE should be configured for normal operation.

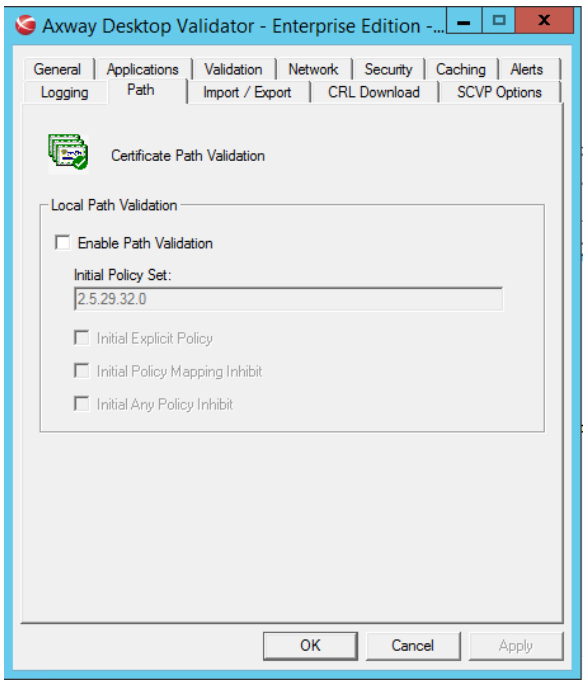
Security tab



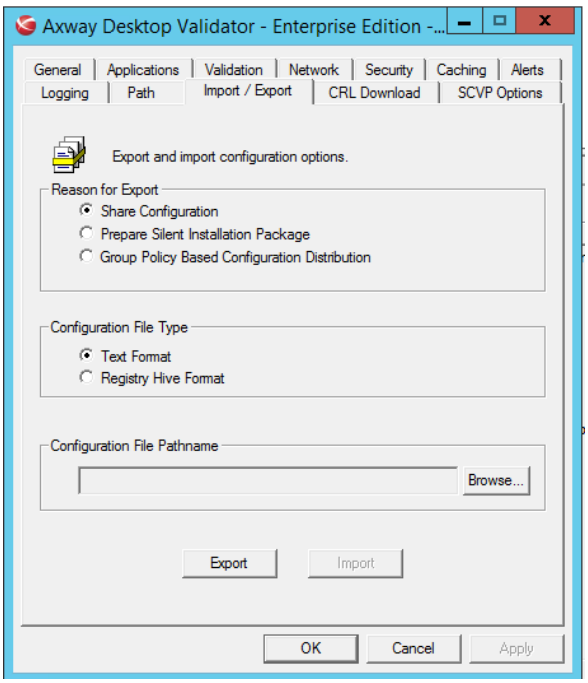
SCVP Options tab



Path tab



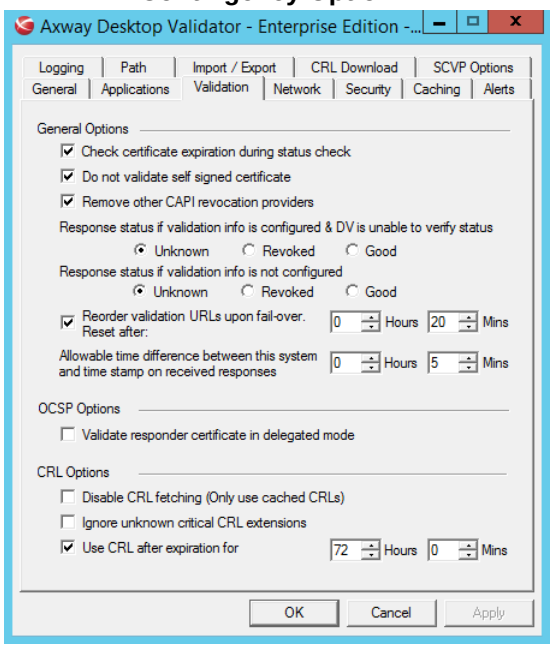
Import / Export tab



F.4 DVE Contingency Option 1

Contingency Option 1 is the preferred option if PIV logon is failing for an extensive amount of user population.

Contingency Option 1



F.4.1 Configuration

The one deviation from the DVE Standard Configuration is made on the *Validation* tab:

- *CRL Options*:
  - The checkbox labeled, "*Use CRL after expiration for*", is selected; ***AND***
  - The corresponding duration of *72 Hours* is configured (adjust duration as necessary).

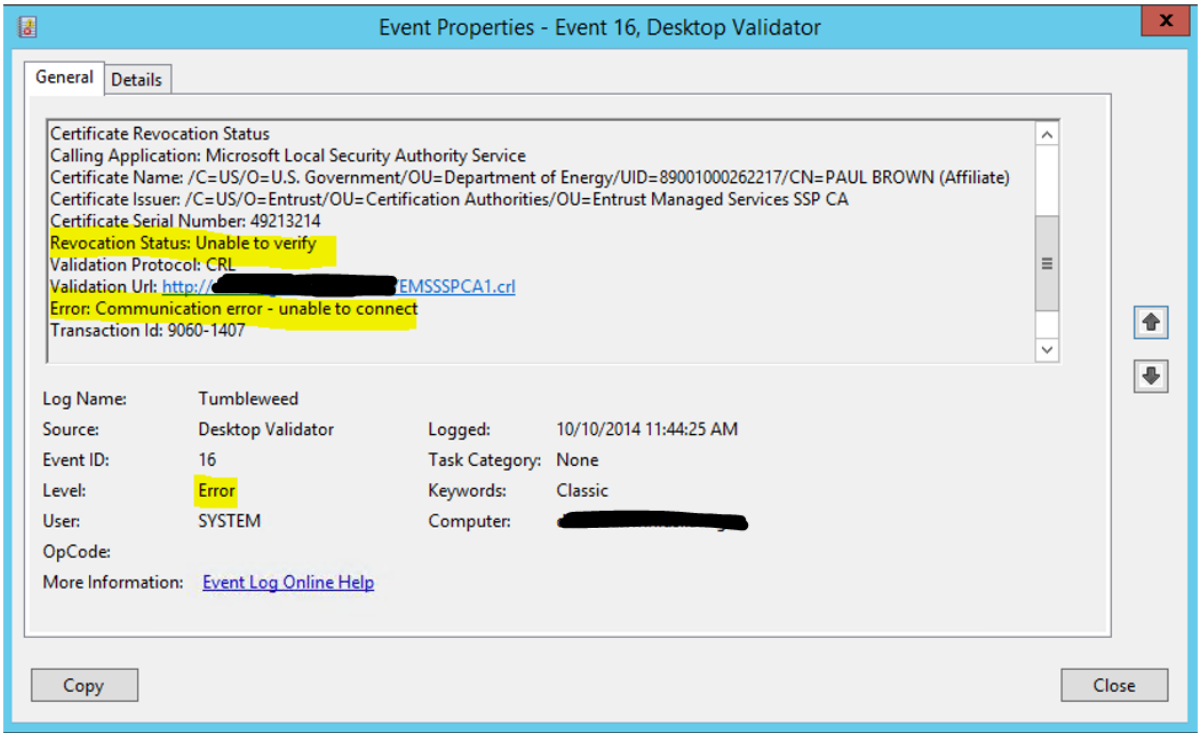
F.4.2 When to use

1. PIV logon is failing because DVE is unable to get a fresh ("non-expired") CRL; ***AND***
2. CRL checking is configured in the *CA-specific Validation Options* for the "offending CA"; ***AND***
3. DVE has a stale ("expired") CRL in the *CRL cache location* (See *Caching* tab in DVE).

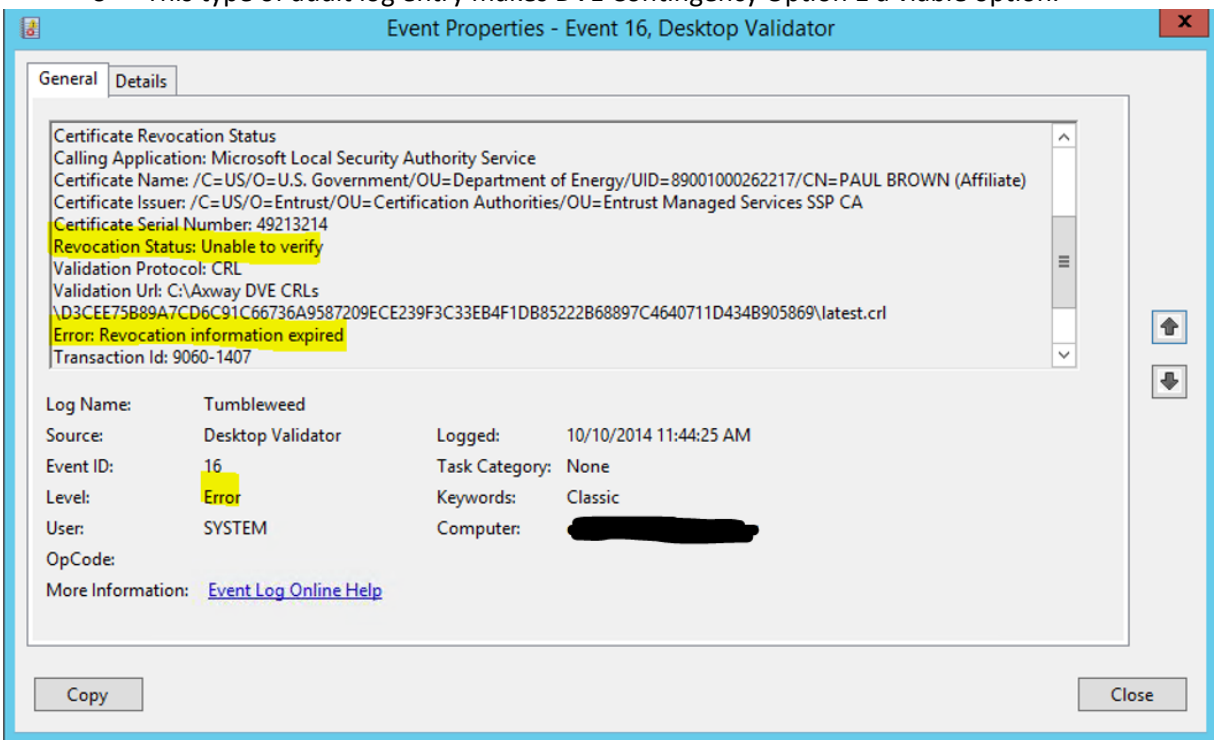
F.4.3 Diagnostics

There will be at least two (2) Tumbleweed audit log Error entries for each certificate (see *Certificate Name* in log entry) being checked by DVE, which can be correlated via the "Transaction Id" in the log:

1. Error *:Event ID 16, Communication error – unable to connect"*
   - Suggests DVE is unable to access the CRL source configured in the *CA-specific Validation Options* for the Certificate Issuer (i.e., the "offending CA").
   - In other words, DVE cannot download the CRL to *CRL cache location.*



2. Error *:Event ID 16, Revocation information expired"*
    - Suggests DVE has a stale ("expired") CRL in its *CRL cache location* for the Certificate Issuer (i.e., the "offending CA").
    - This type of audit log entry makes DVE Contingency Option 1 a viable option.

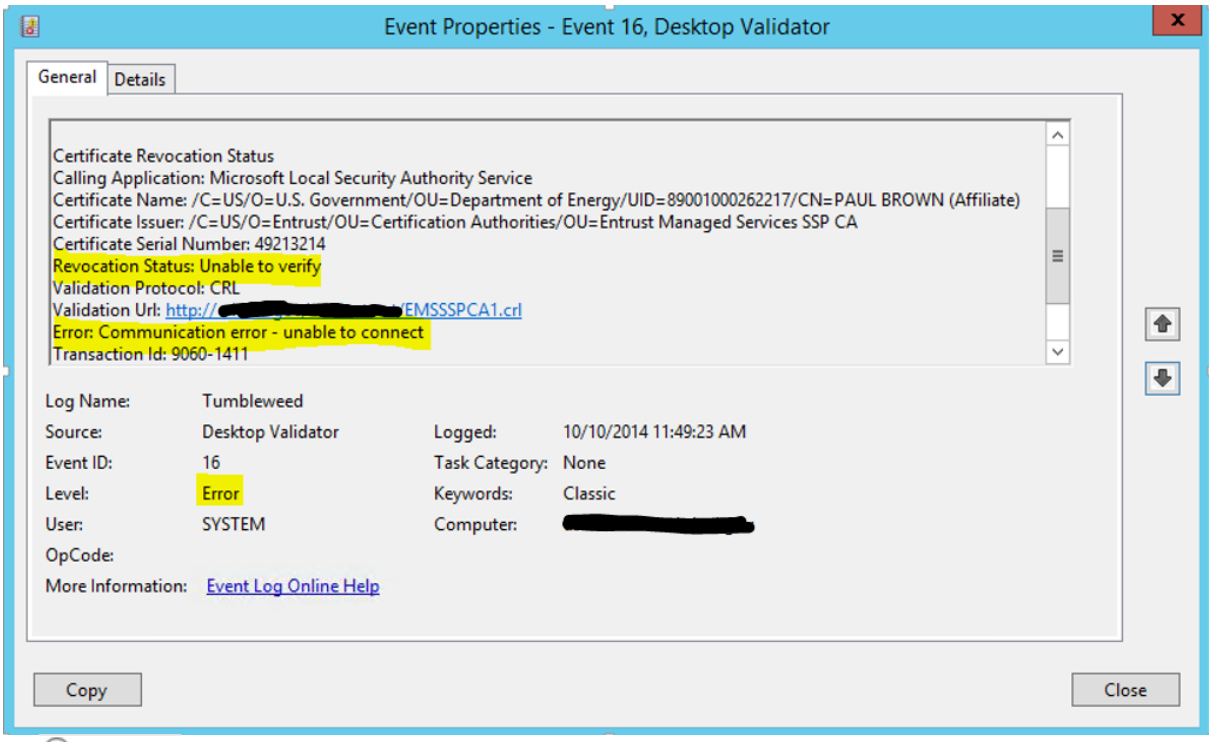


F.4.4 Benefit

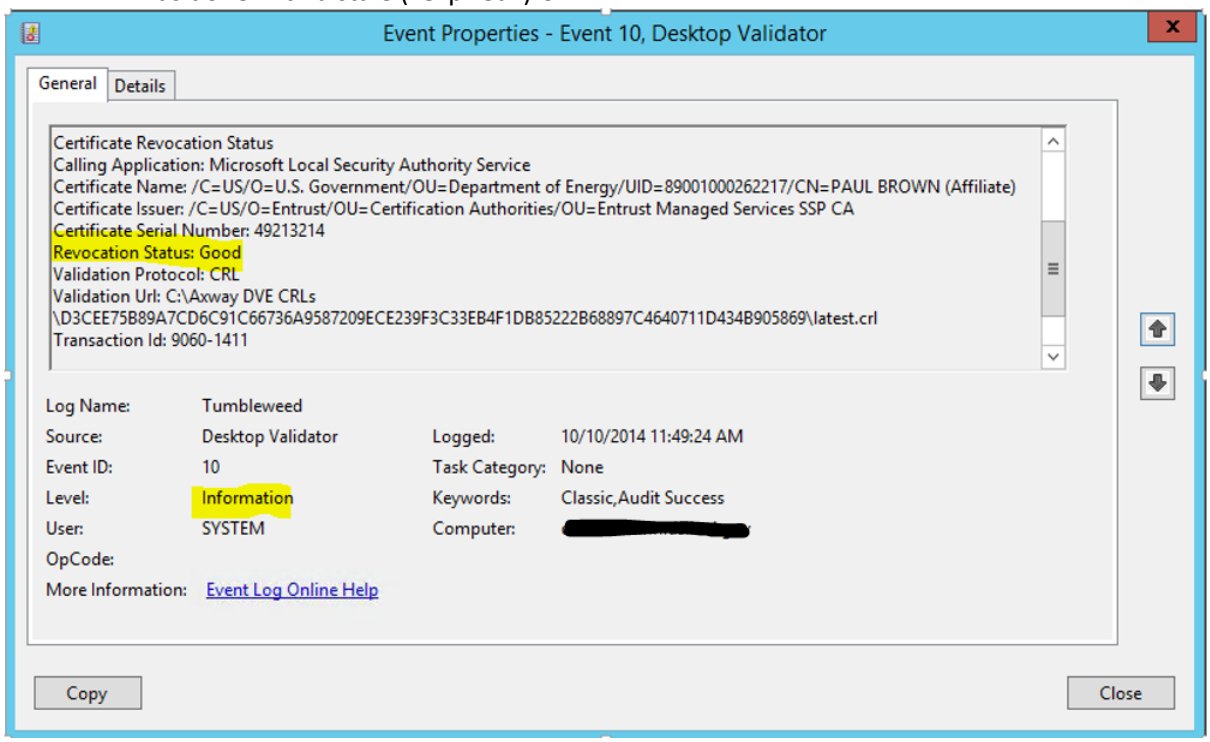
1. Users may continue to logon with their PIV Card while administrators diagnose and resolve the issue that is causing DVE to not get fresh ("non-expired") CRLs.
2. Revocation status checking is still being performed against a CRL, preventing known revoked certificates from being used for logon to the network.
3. DVE continues to check for a "fresh" CRL and will use it once it becomes available.

After applying Configuration Option 1, there will continue to be at least two (2) Tumbleweed audit logs: one (1) Error and one (1) Information. These are generated for each certificate (see *Certificate Name* in log entry) being checked by DVE until the issue has been resolved. The two (2) audit logs can be correlated via the "Transaction Id" in each log.

1. Error *:Event ID 16, Communication error – unable to connect"*
    - Suggests DVE **is trying but still unable** to access the CRL source configured in the *CA-specific Validation Options* for the Certificate Issuer (i.e., the "offending CA").



2. Information *:Event ID 10, Revocation status"*
    - Suggests DVE **performed** a revocation status check using the CRL in its *CRL cache*.
    - It looks like a normal record; however by correlating this audit record with the previous record that shows a failed attempt to obtain a CRL, the conclusion is that revocation status checking was done with a stale ("expired") CRL.



F.4.5 Risk and Mitigation

There is a risk that a Domain Controller would allow a revoked certificate to be used for logon if the certificate was revoked after the CRL was published by its CA and downloaded to DVE's *CRL cache location* on the DC. However, the number of certificates that could be used is significantly small. The number of certificates posing a risk to the network:

1. Is constrained to those who have had their PIV revoked since the last time DVE received an updated CRL
2. Is further limited to the local user population, and even then, to those who have had their PIV revoked since the last time DVE received an updated CRL

This contingency allows for revocation status checking for the greater majority versus performing revocation status checking for none. Furthermore, DVE is configured to only validate certificates issued from CAs that the organization trusts. All other certificates are denied; therefore, logon is only available using certificates (or PIVs) that are from a trusted source. Lastly, DVE continues to check for a fresh ("non-expired") CRL and uses it once it becomes available.

F.5 DVE Contingency Option 2

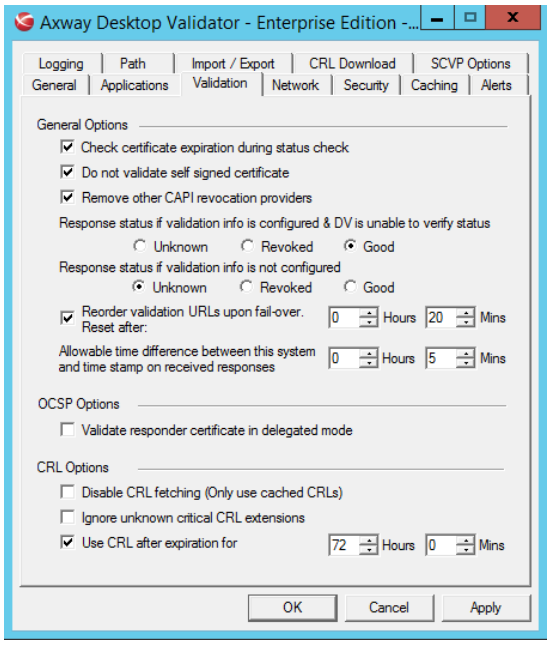
DVE Contingency Option 2 should be used only if DVE Contingency Option 1 doesn't meet operational needs while troubleshooting the issue. With this configuration, DVE defaults to "Good" if a status check cannot be rendered for one of the configured CAs in the *"CA-specific Validation Options"* on the *General* tab.

F.5.1 Configuration

The deviations from the DVE Standard Configuration are made on the *Validation* tab:

- *General Options*:
  - The radio button *"Good"* is selected for "*Response status if validation info is configured & DV is unable to verify status*"
- *CRL Options*:
  - The checkbox labeled, "*Use CRL after expiration for*", is selected; ***AND***
  - The corresponding duration of *72 Hours* is configured

Contingency Option 2



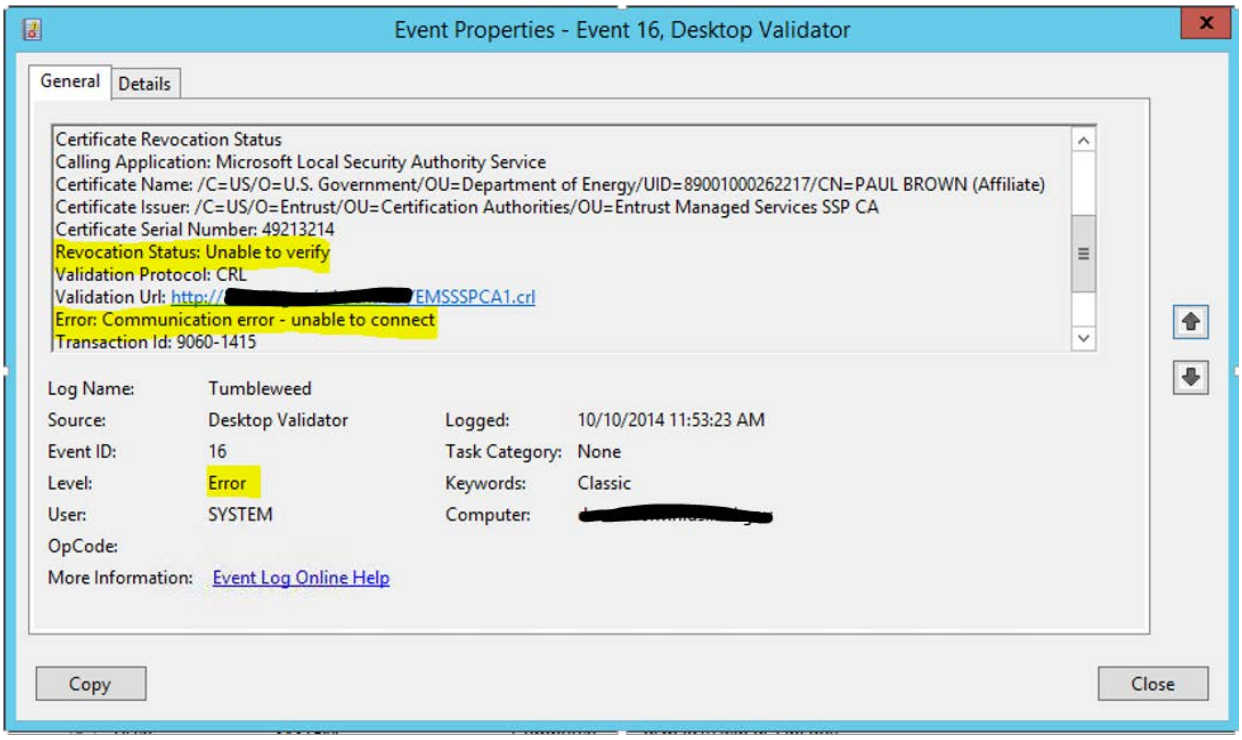
F.5.2 When to use

1. PIV logon is failing because DVE is unable to successfully validate certificates for one or more CAs (i.e., certificate issuers) configured in the *CA-specific Validation Options* of the *General* tab; ***AND***
2. DVE does not have a stale ("expired") CRL in the *CRL cache location* (See *Caching* tab in DVE) for one or more of the "offending" CAs; ***AND***
3. All other revocations status options (e.g., OCSP) are not successful (or not configured) for each of the "offending" CAs in the *CA-specific Validation Options* configured in the *General* tab

F.5.3 Diagnostics

For CRL failures, there will be only one (1) Tumbleweed audit log Error entry for each certificate (see *Certificate Name* in log entry) being checked by DVE:

1. Error :*Event ID 16, Communication error – unable to connect"*
    - This indicates that DVE is unable to access the CRL source configured in the *CA-specific Validation Options* for the Certificate Issuer (i.e., the "offending CA").
    - In other words, DVE is unable to download the CRL to its *CRL cache location*.
    - Moreover, the fact there are no additional audit records indicating revocation data has expired, it means that (1) the DVE has never obtained and used a CRL before now*;* or (2) a person or process deleted the CRL(s) from the *CRL cache location.*



F.5.4 Benefit

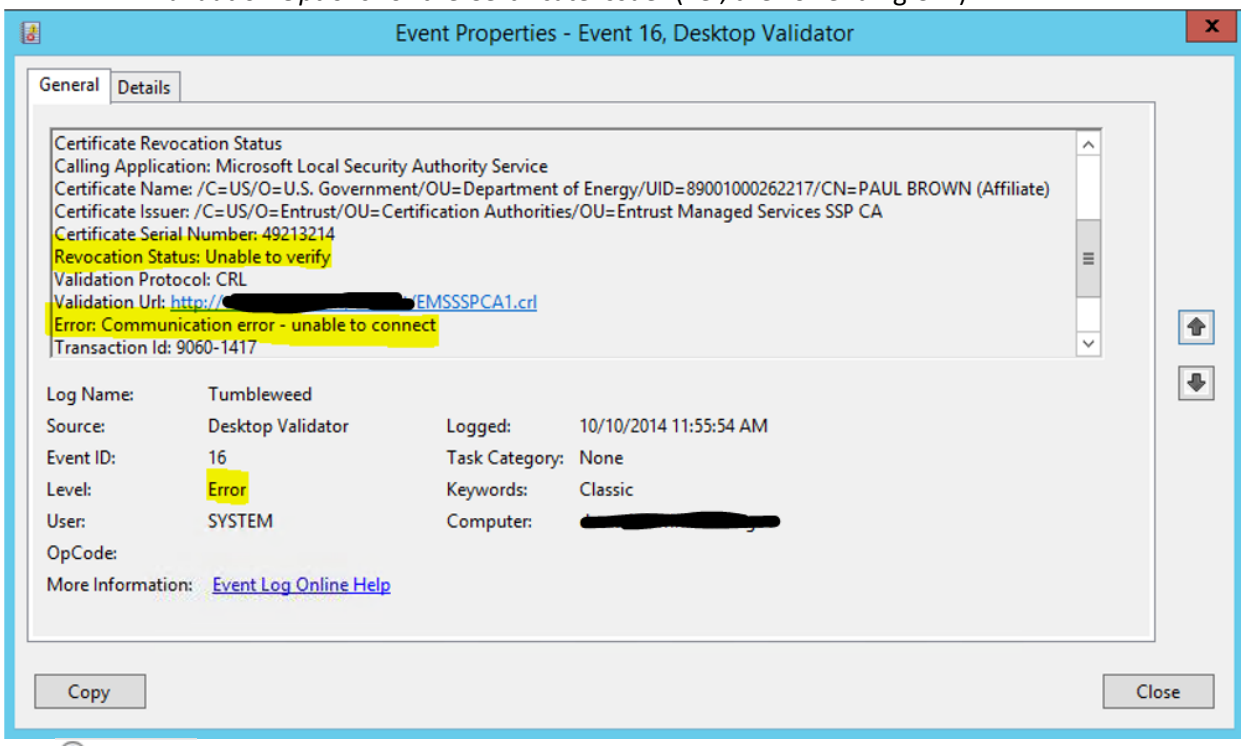
This option retains all the benefits of Contingency Option 1 but also addresses revocation status checking failures beyond stale (or "expired") CRLs.

1. Users may continue to logon with their PIV Card while administrators diagnose and resolve the issue that is causing DVE to not perform revocation status checking as expected.
2. DVE continues to performing revocation status checks for certificates issued by CAs for which the DVE is able, and defaults to "Good" if a status check cannot be rendered for one of the configured CAs in the *"CA-specific Validation Options"* on the *General* tab.
3. If a stale ("expired) CRL is available, DVE will perform revocation status checking against it for the time period configured, preventing known revoked certificates from being used for logon.
4. DVE continues to check for a "fresh" CRL and will use it once it becomes available.

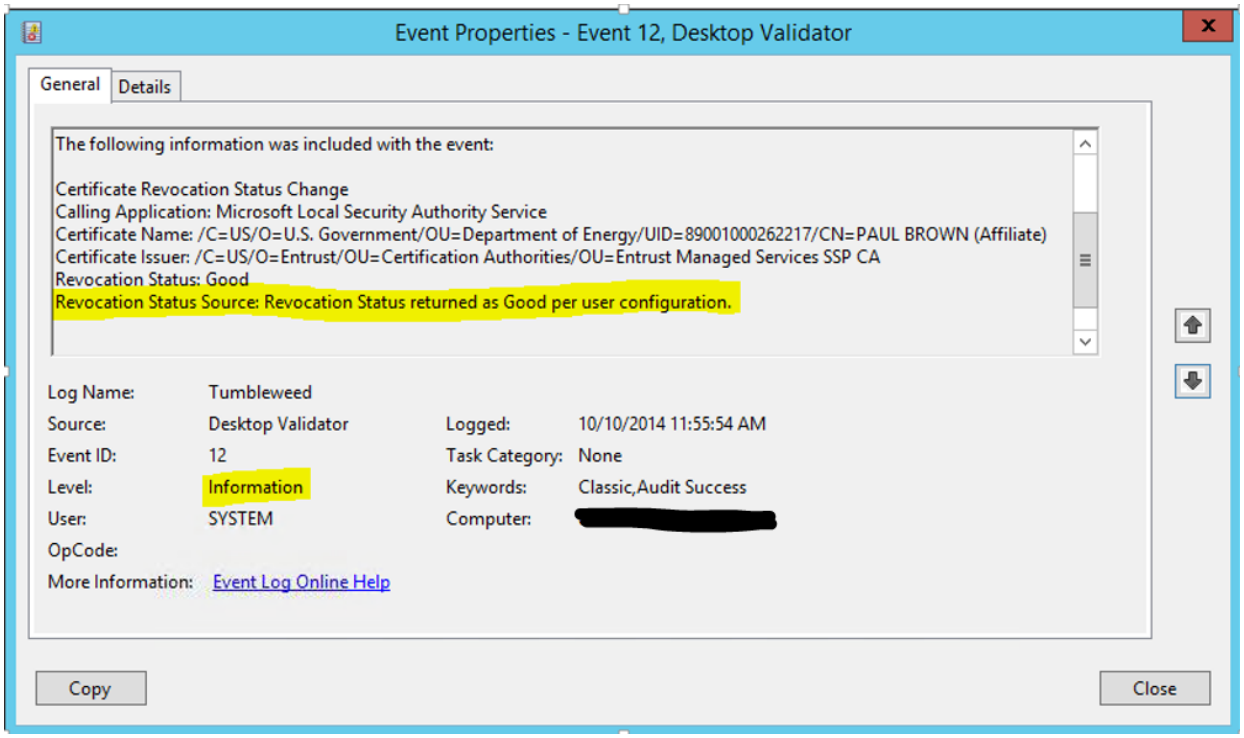
After applying DVE Contingency Option 2, there will continue to be at least two (2) Tumbleweed audit logs generated for each certificate (see *Certificate Name* in log entry) being checked by DVE until the issue has been resolved:

1. Error :*Event ID 16, Communication error – unable to connect"*

- Suggests DVE **is trying but still unable** to access the CRL source configured in the *CA-specific Validation Options* for the Certificate Issuer (i.e., the "offending CA").



2. Information *:Event ID 12, Revocation status"* indicating DVE **defaulted to "Good"**.
   - Unfortunately, the record does not contain the corresponding *Transaction Id* to correlate it with the previous record that shows a failed attempt to obtain a CRL. A request to the Vendor has been made to include this information in the record.



F.5.5 Risk and Mitigation

With this configuration, there is a risk that a Domain Controller would allow a revoked certificate to be used for logon if the certificate was revoked:

1. After the CRL was published by its CA and downloaded to DVE's *CRL cache location* on the DC (See Contingency Option 1); ***or subsequently***
2. From one of the CAs configured in the *CA-specific Validation Options* in the *General* tab and DVE is unable to render a certificate status check for some reason

DVE continues to performing revocation status checks for certificates issued by CAs for which the DVE is able, and only defaults to "Good" if a status check cannot be rendered for one of the configured CAs in the *"CA-specific Validation Options"* on the *General* tab. Revocation status checking is performed when possible versus not performing revocation status checking at all. Furthermore, DVE is configured to only validate certificates issued from CAs that the organization trusts. All other certificates are denied; therefore, logon is only available using certificates (or PIVs) that are from a trusted source. DVE continues to attempt a revocation status check as configured in the *CA-specific Validation Options* in the *General* tab prior to using the default "Good" status.

F.6 DVE Contingency Option 3

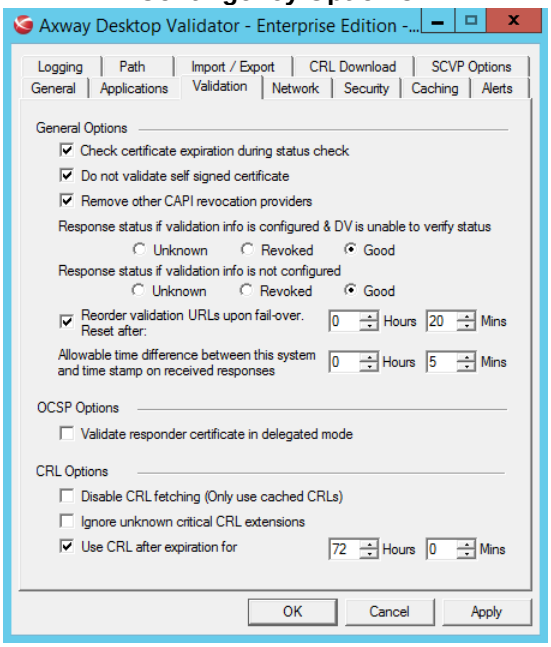
DVE Contingency Option 3 should not be needed if the *CA-specific Validation Options* on the *General* tab is configured with all the requisite CAs. With this configuration, DVE defaults to "Good" for any certificate for which it cannot render a status check.

F.6.1 Configuration

The deviations from the DVE Standard Configuration are made on the *Validation* tab:

- *General Options*:
  - The radio button *"Good"* is selected for "*Response status if validation info is configured & DV is unable to verify status"*
  - The radio button *"Good"* is selected for "*Response status if validation info is not configured"*
- *CRL Options*:
  - The checkbox labeled, "*Use CRL after expiration for"*, is selected; ***AND***
  - The corresponding duration of *72 Hours* is configured

Contingency Option 3



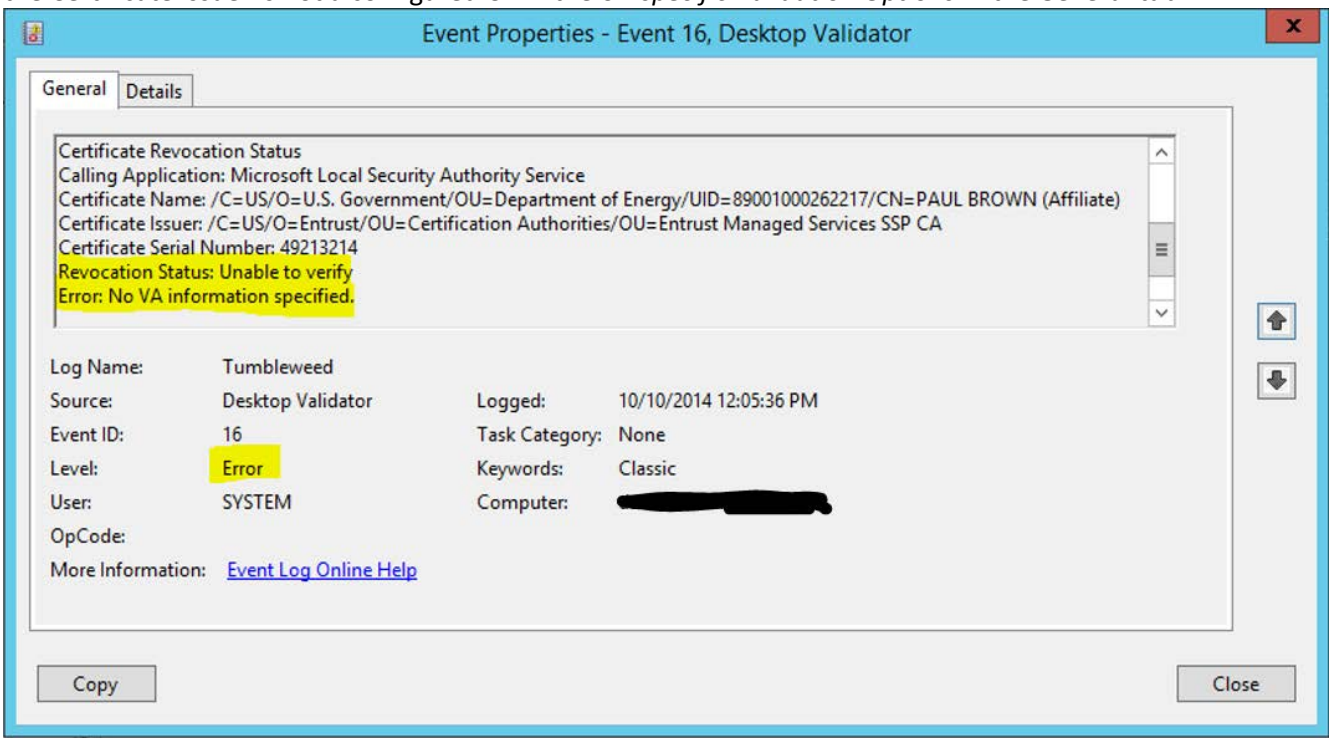
F.6.2 When to use

1. PIV logon is failing and the Windows AD Administrator believes it might be related to DVE not successfully validating a certificate; ***AND***
2. DVE Contingency Options 1 & 2 were tried, but PIV logon continues to fail

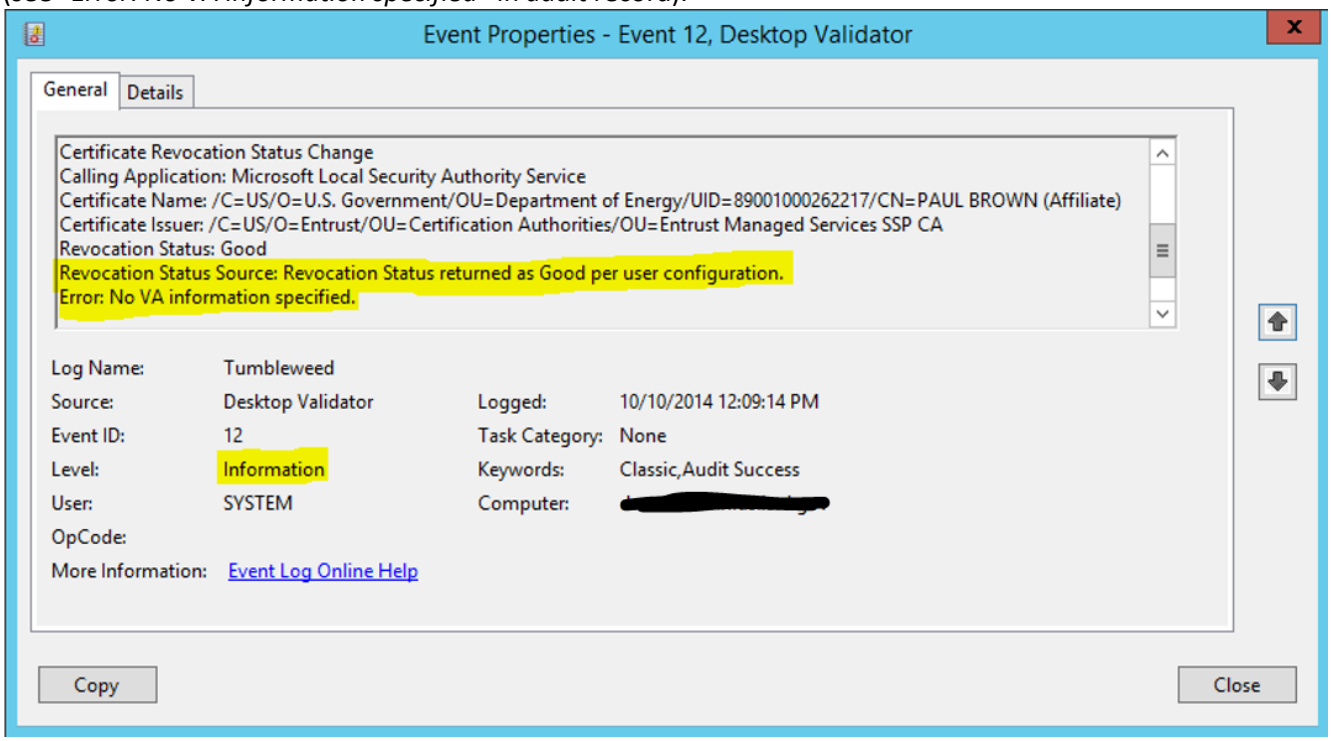
This option should only be implemented for the time period to assess whether or not PIV logon is successful.

F.6.3 Diagnostics

There will be one (1) Tumbleweed audit log Error entry for each certificate (see *Certificate Name* in log entry) being checked by DVE. The log entry will have "*Error: No VA information specified*", which means that the Certificate Issuer is not a configured CA in the *CA-specific Validation Options* in the *General* tab.



If PIV logon is successful after applying DVE Contingency Option 3, then the "offending" CA is not configured in the *CA-specific Validation Options* on the *General* tab, as shown in the Tumbleweed Information audit record (see "*Error: No VA information specified"* in audit record).



If PIV logon continues to fail, then there is a fundamental problem with DVE or the failed logons are not related to revocation status checking.

F.6.4 Risk and Mitigation

The risks and mitigations are the same as described for DVE Contingency Option 2.

If PIV logon is successful, then that means that one or more CAs (i.e., certificate issuers) associated with the certificate is not configured in the *CA-specific Validation Options* on the *General* tab. For logon to have been successful, the Windows AD had to have been configured to accept (or trust) the CA certificates but the configuration was not propagated to the DVE. This typically happens when AD is updated with a change to existing PIV Card infrastructure by the PIV Card issuer or to accommodate a new PIV Card issuer is introduced to the environment (e.g., Department of State employee comes to organization and requires logon access using their agency issued PIV). Thus, the DVE will be updated and the DVE can return to normal standard operational configuration.

If PIV logon is still not successful, then the DVE can return to normal standard operational configuration and other troubleshooting is required.

This option should only be implemented for the time period to assess whether or not PIV logon is successful.

F.7 Scenarios of Operational Disruptions and the Recommended Contingency Option

This section describes multiple scenarios associated with revocation status checking that could cause operational disruptions to the PIV logon process. The table below:

- Describes each operational scenario;
- Identifies the potential audit logs generated in the Event Viewer application log called, Tumbleweed;
- Suggests the preferred contingency option in Appendix F to implement; and
- Provides a high-level rationale to communicate to decision makers.

	Operational Disruption Scenario	Tumbleweed Audit Logs	Contingency			
			Option 1	Option 2	Option 3	Rationale
1)	1. The Local CRL Repository (LCR): a. Has "expired" CRLs; ***AND*** b. Is not getting fresh ("non-expired) CRLs from the target source (source is down, network or internet issues, etc.) 2. DVE: a. Is configured for only CRLs for the certificate issuer in *CA-Specific Validation Options*; ***AND*** b. Is not getting fresh ("non-expired") CRLs from the LCR; ***BUT*** c. Has stale ("expired") CRLs in the *CRL cache location* (See *Caching* tab in DVE)	1. Figure 4: Revocation information expired	**Preferred** F.4			Since DVE has cached CRLs, use them even though they are stale ("expired"). Continue to use stale CRLs while troubleshooting why the Local CRL Repository is not able to get fresh ("non-expired") CRLs from the target source. This allows for revocation status checking for the greater majority versus performing revocation status checking for none. This contingency allows for PIV logon to continue functioning versus resorting to other credentials for logon.
2)	1. The LCR is unavailable (down, disconnected, etc.); 2. DVE: a. Is configured for only CRLs for the certificate issuer in *CA-Specific Validation Options*; ***AND*** b. Is unable to get fresh ("non-expired") CRLs from the LCR; ***BUT*** c. Has stale ("expired") CRLs in the *CRL cache location* (See *Caching* tab in DVE)	1. Figure 3: Communication error – unable to connect (CRL) 2. Figure 4: Revocation information expired	**Preferred** F.4			Since DVE has cached CRLs, use them even though they are stale ("expired"). Continue to use stale CRLs while troubleshooting why the Local CRL Repository is down or not available to the Domain Controllers. This allows for revocation status checking for the greater majority versus performing revocation status checking for none. This contingency allows for PIV logon to continue functioning versus resorting to other credentials for logon.

	Operational Disruption Scenario	Tumbleweed Audit Logs	Contingency			
			Option 1	Option 2	Option 3	Rationale
3)	1. DVE: a. Cannot get a CRL for the certificate issuer in *CA-Specific Validation Options*; ***AND*** b. Is configured for only CRLs for this certificate issuer; ***AND*** c. Does not have a stale ("expired") CRL in the *CRL cache location* (See *Caching* tab in DVE)	1. Figure 3: Communication error – unable to connect (CRL)		**Preferred** F.5		This temporary configuration allows PIV logon to function while administrators troubleshoot why the Domain Controllers are unable to get CRLs. This contingency allows for PIV logon to continue functioning versus resorting to other credentials for logon. The Domain Controllers are configured to allow only specific credentials that are issued by trusted federal entities.
4)	1. DVE: a. Cannot get to the OCSP configured for the certificate issuer in *CA-Specific Validation Options*; ***AND*** b. Is configured for only OCSP for this certificate issuer	1. Figure 5: Communication error - unable to connect (OCSP)		**Preferred** F.5		This temporary configuration allows PIV logon to function while administrators troubleshoot why the Domain Controllers are unable to get to the OCSP to validate PIV cards. This contingency allows for PIV logon to continue functioning versus resorting to other credentials for logon. The Domain Controllers are configured to allow only specific credentials that are issued by trusted federal entities.
5)	1. DVE: a. Is configured for OCSP and CRLs for the certificate issuer in *CA-Specific Validation Options*; ***AND*** b. Cannot get to the OCSP; ***AND*** c. Cannot get a fresh ("non-expired) CRL; ***BUT*** d. Has a stale ("expired") CRL in the *CRL cache location* (See *Caching* tab in DVE)	1. Figure 5: Communication error - unable to connect (OCSP) 2. Figure 3: Communication error – unable to connect (CRL) 3. Figure 4: Revocation information expired	**Preferred** F.4			Since DVE has cached CRLs, use them even though they are stale ("expired"). Continue to use stale CRLs while troubleshooting why the Local CRL Repository is not able to get fresh ("non-expired") CRLs from the target source. This allows for revocation status checking for the greater majority versus performing revocation status checking for none. This contingency allows for PIV logon to continue functioning versus resorting to other credentials for logon.

	Operational Disruption Scenario	Tumbleweed Audit Logs	Contingency			
			Option 1	Option 2	Option 3	Rationale
6)	1. DVE: a. Is configured for OCSP and CRLs for the certificate issuer in *CA-Specific Validation Options*; ***AND*** b. Cannot get to the OCSP; ***AND*** c. Cannot get a fresh ("non-expired) CRL; ***AND*** d. Does not have a stale ("expired") CRL in the *CRL cache location* (See *Caching* tab in DVE)	1. Figure 5: Communication error - unable to connect (OCSP) 2. Figure 3: Communication error – unable to connect (CRL)		**Preferred** F.5		This temporary configuration allows PIV logon to function while administrators troubleshoot why the Domain Controllers are unable to get to the CRLs and OCSP to validate PIV cards. This contingency allows for PIV logon to continue functioning versus resorting to other credentials for logon. The Domain Controllers are configured to allow only specific credentials that are issued by trusted federal entities.
7)	1. Logon is failing and all there is no indication why in the audit records				**Preferred** F.6	This temporary configuration will help administrators determine if revocation data (or the lack of) "in general" is the cause for PIV logon failures. This contingency allows for PIV logon to continue functioning versus resorting to other credentials for logon. The Domain Controllers are configured to allow only specific credentials that are issued by trusted federal entities.

F.8 Catalog of Tumbleweed Audit Logs

Figure 3: Communication error – unable to connect (CRL) *(see F.4.3, F.5.3 for more details)*

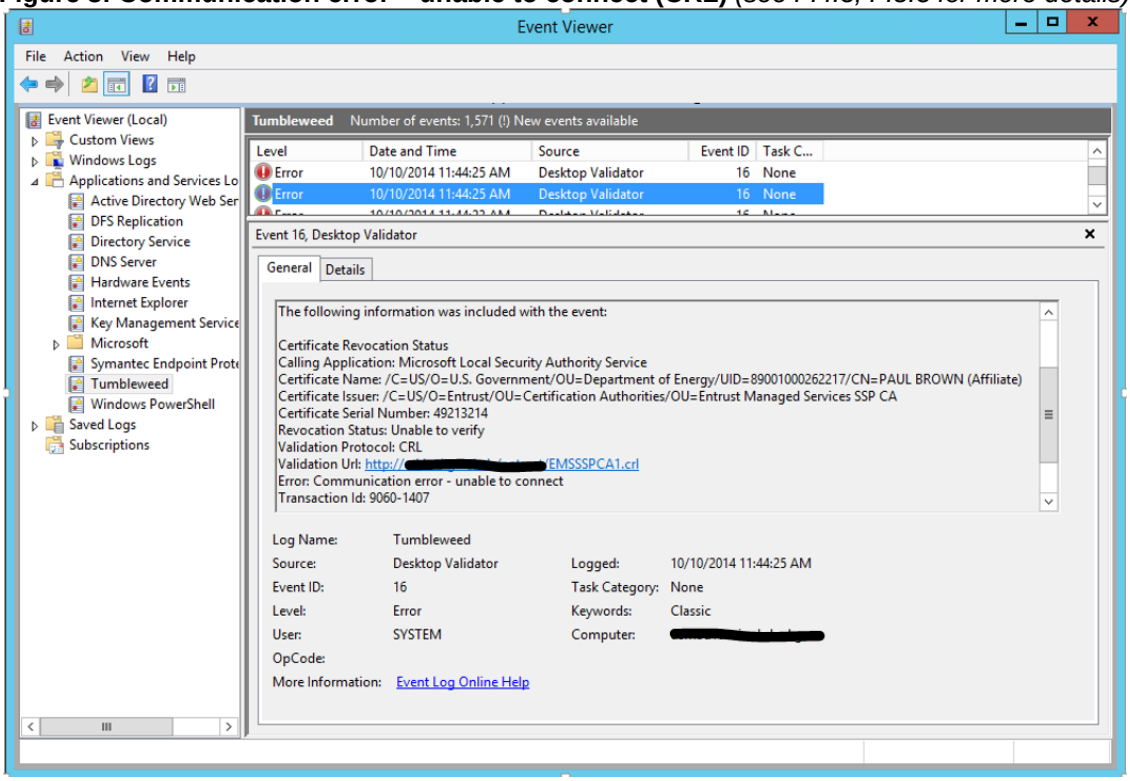


Figure 4: Revocation information expired *(see F.4.3 for more details)*

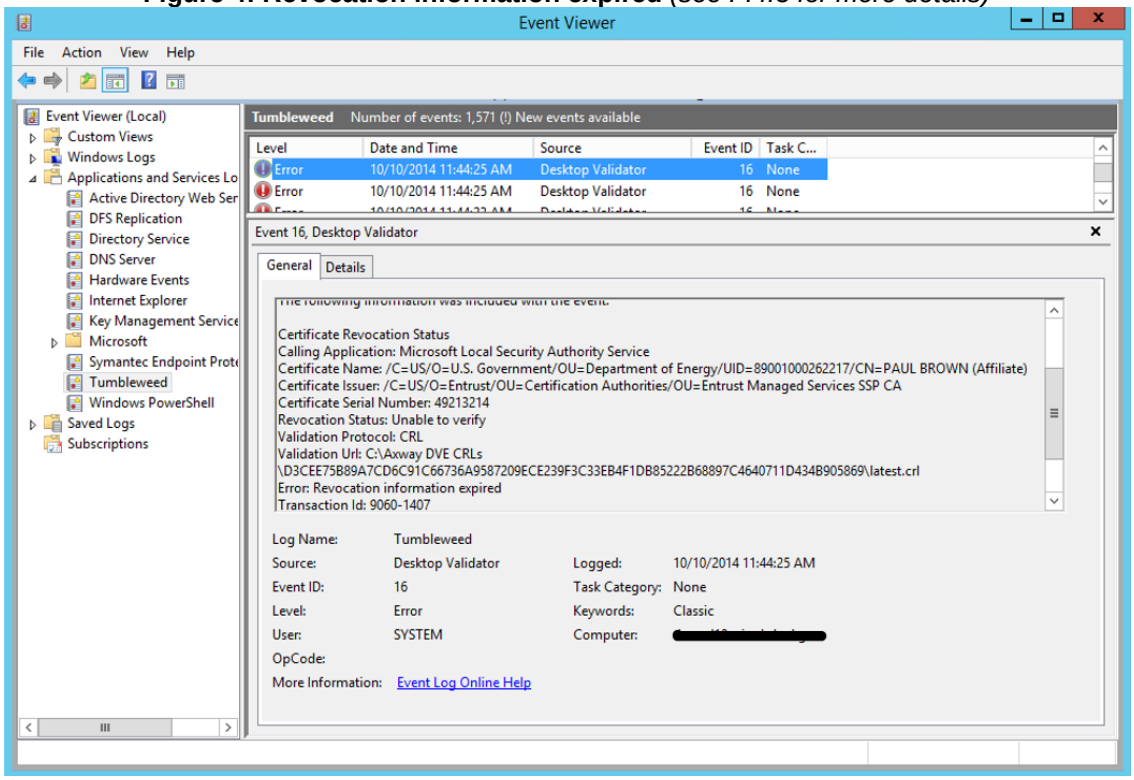


Figure 5: Communication error - unable to connect (OCSP)

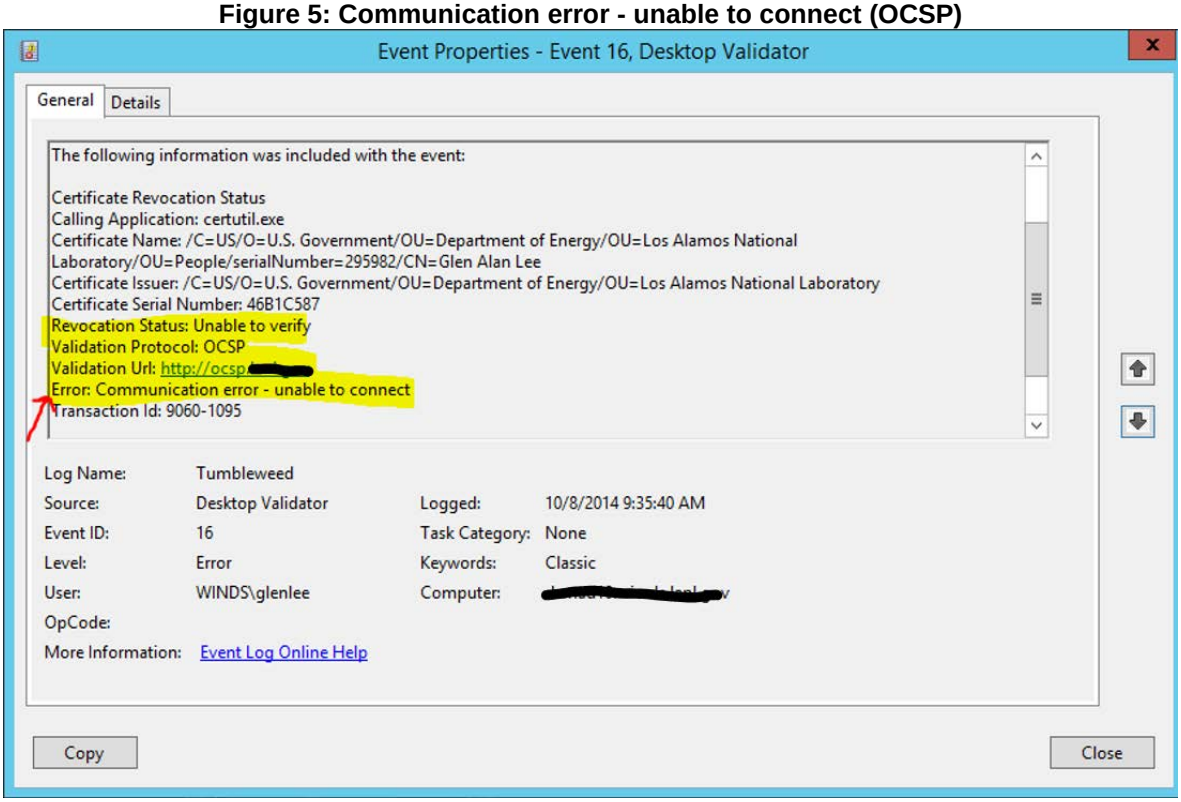


Figure 6: CRL Download Scheduler Error - Communication error

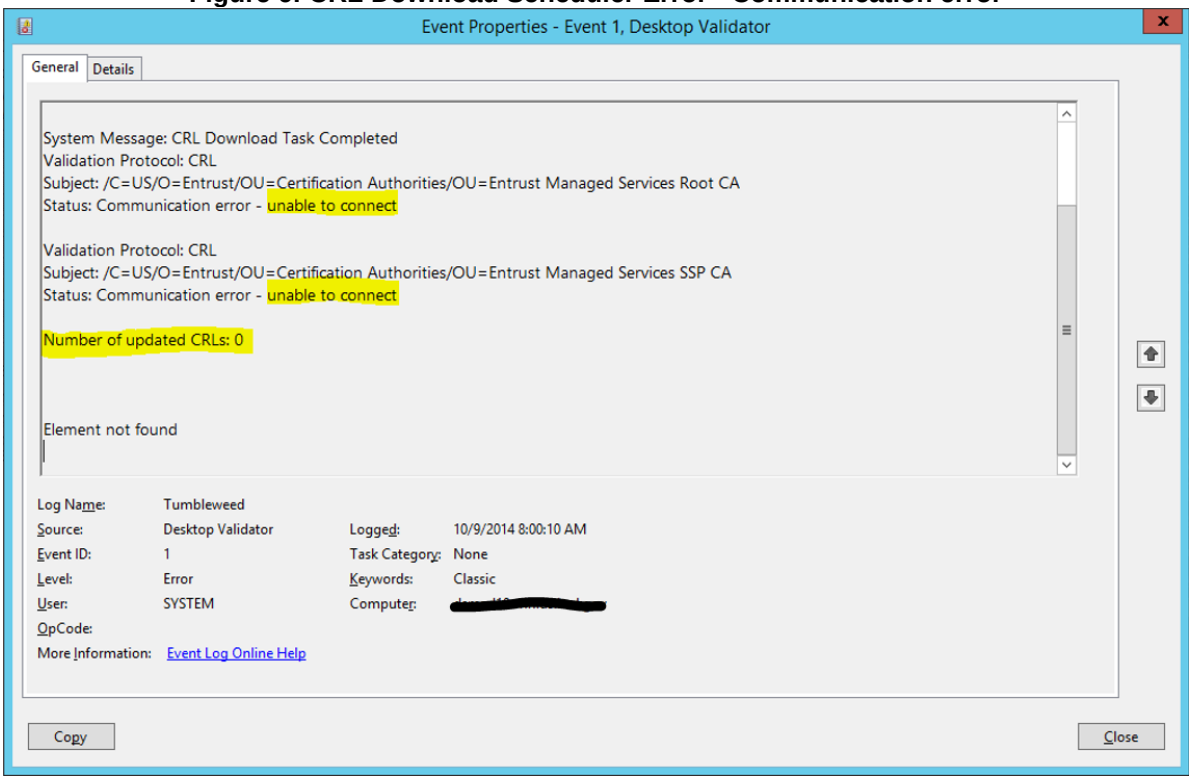
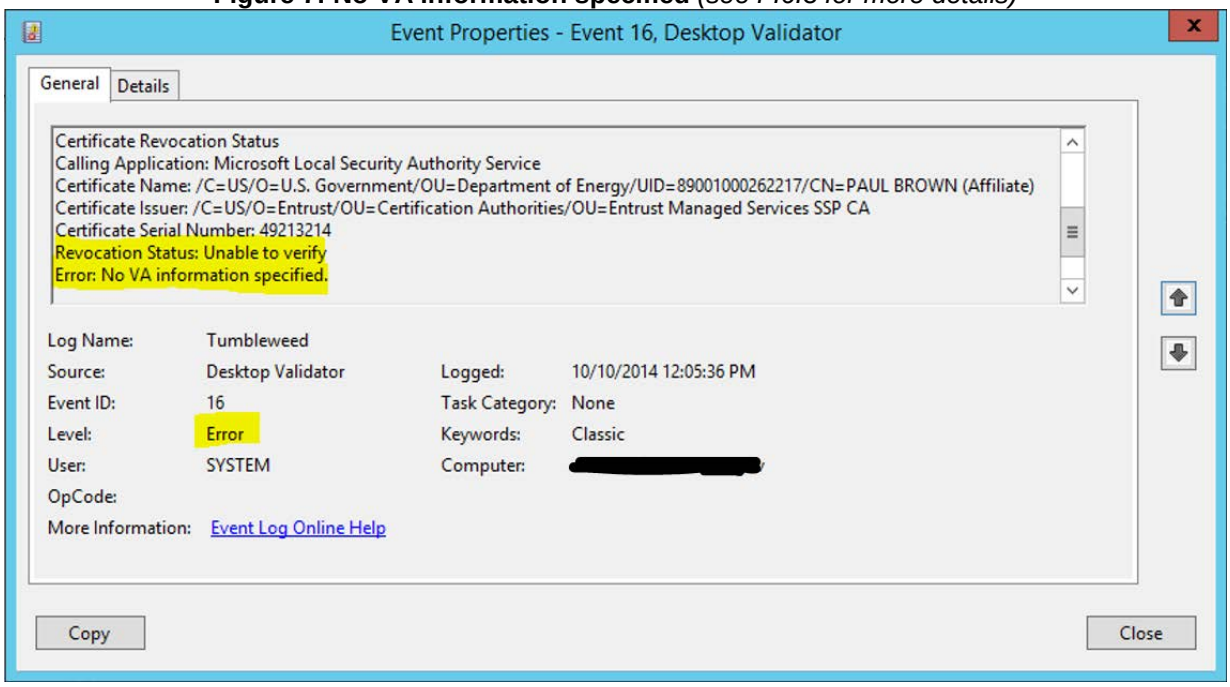


Figure 7: No VA information specified *(see F.6.3 for more details)*



Appendix G Checklist

Check	#	Item	Sections	Comments
	1.	Installed Microsoft Enterprise CA per § 2.1	2.1	
	2.	Added both the Entrust Root and SSP CA certificates to enterprise AD stores per § 2.2	2.2	
	3.	Configured auto-enrollment GPO for DC certificate issuance per § 2.3	2.3	
	4.	Verified DCs have certificates issued from the OLT PKI per § 2.3	2.3	
	5.	Applied GPO containing registry modifications to DCs to ignore UPN Mapping per § 2.4	2.4	
	6.	Applied PIN change hotfix and associated GPO containing registry modifications to pilot computers per § 3.2	3.2	
	7.	Applied the GPO to make registry modifications to pilot computers to enable logon interface to support PIV logon via certificate mapping per § 3.1	3.1	
	8.	Applied the GPS containing the registry modifications to pilot computers to “not lock” on smart card removal per § 3.2	3.2	
	9.	Connected smart card reader to pilot computers per § 3.3	3.3	
	10.	Configured test user accounts with PIV certificate per § 4.1.2	4.1.2	
	11.	Installed Local CRL Repository per § 2.5.2	2.5.2	
	12.	Copied DVE Installation and Configuration Files to \\[domain]\NETLOGON\DVE	2.5.3.2	
	13.	Installed Axway DVE on all DCs and configured with *Standard Configuration* per § 2.5.3.2	2.5.3.2	
	14.	Created DVE GPO, *Axway_DVE_Configuration_for_DCs*, per § 2.5.3.3	2.5.3.3	