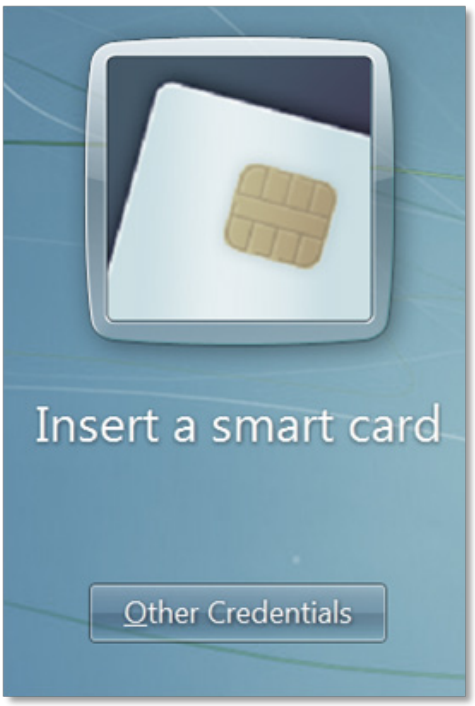
Smart Card Two-Factor Authentication

This white paper provides information about supported Two-Factor Authentication applicable to DeltaV™ Systems.



DELTAV™

EMERSON™
Process Management

Contents

Introduction

The combination of a smart card and a personal identification number (PIN) provides Two-Factor Authentication, where two items are needed: something physical the user has (a smart card) and something the user knows (a PIN). Since something physical and something non-physical are both required, the result is a much more secure means of authenticating users.

Logins based on user names and passwords are not as secure as Two-Factor Authentication since user names are easily determined—they are essentially single-factor authentication (i.e., something you know—the password or PIN. To make the systems more secure, a physical entity is added to the login requirement—a smart card. A smart card is a badge-like device that stores user credentials. These credentials can include name, Microsoft® Windows certificates, and card lifetime.

DeltaV Logon – Smart Card Optional

The DeltaV logon dialog has been modified to allow the user to check the Use Smart Card Logon checkbox, which removes the user name entry and directs the user to insert a smart card and enter a PIN. (See Figure 1.)

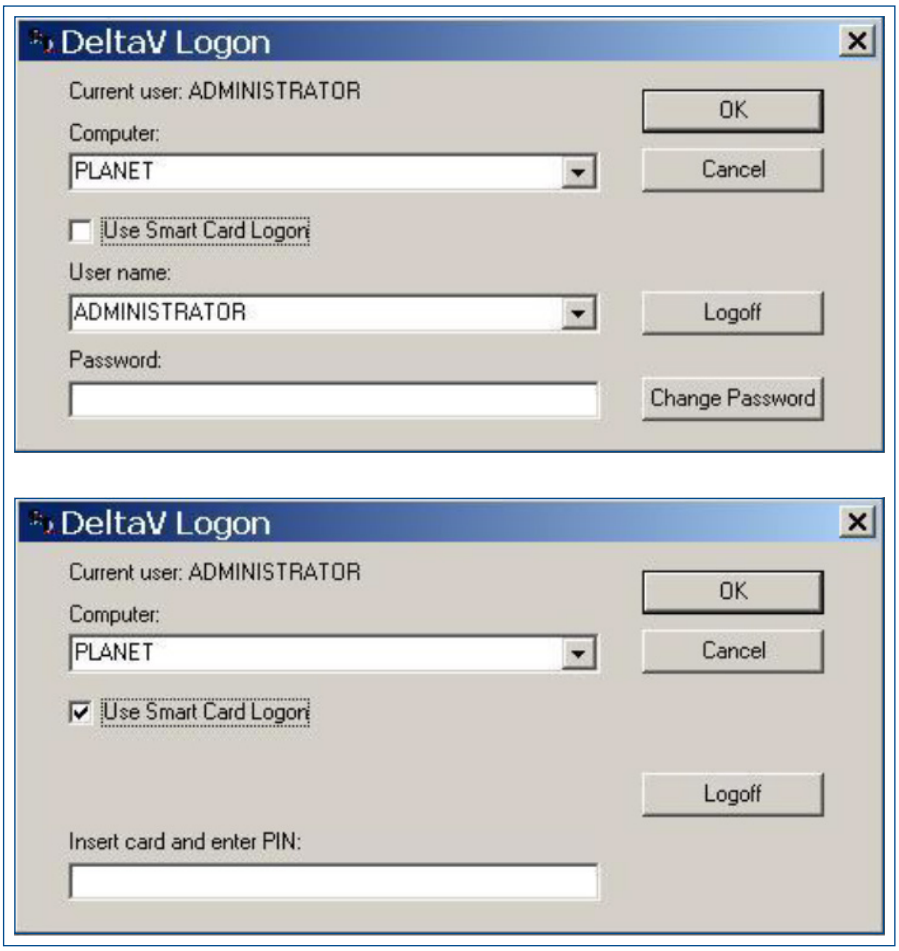


Figure 1 – DeltaV Logon Smart Card optional

DeltaV FlexLock and DeltaV Logon – Smart Card Required

FlexLock has a new menu option that DeltaV administrators and Windows administrators have the privilege to select that requires users to use a Smart Card and PIN rather than a username and password. When the Smart Card Required option is selected, the DeltaV logon dialog changes to prompt the user to only insert a smart card and enter a PIN. This setting is set for each workstation and is preserved during DeltaV upgrades. (See Figures 2 and 3.)

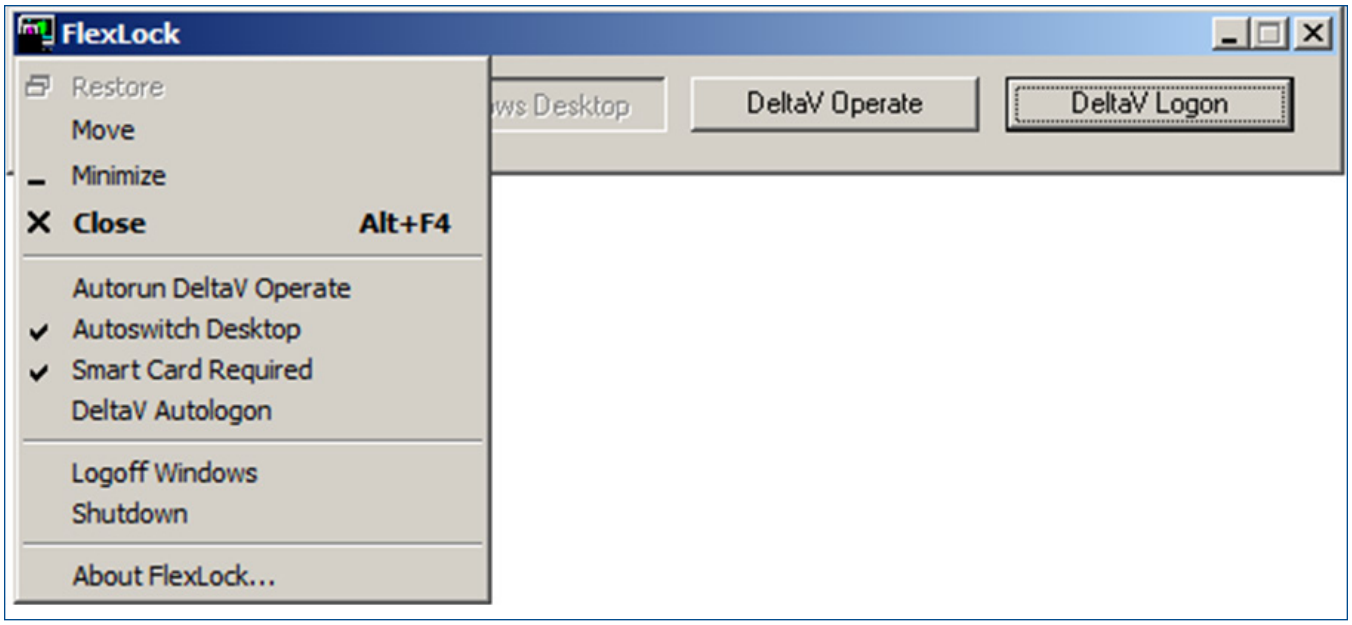


Figure 2 – DeltaV FlexLock Smart Card Required option

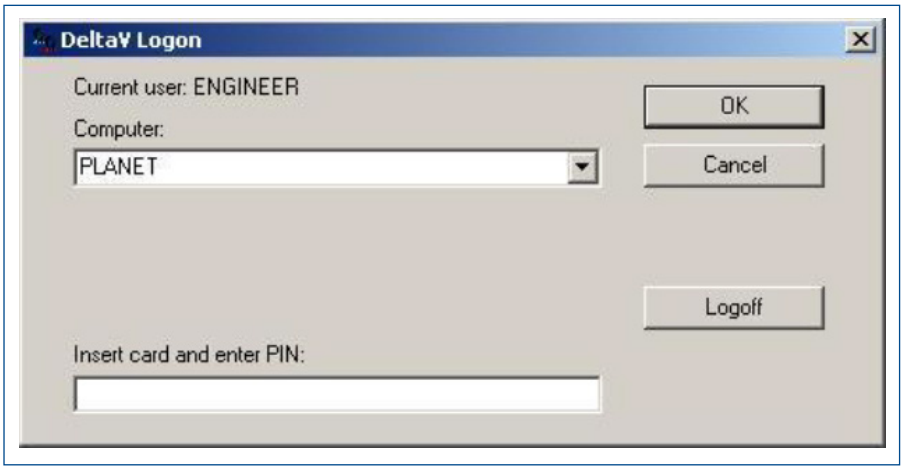


Figure 3 – DeltaV Logon Smart Card required

Windows Remote Desktop Settings

Smart Card credentials can be transferred through the Windows Remote Desktop application. If you are using Smart Cards as a means of ensuring physical presence at a specific workstation, then the workstation settings must be changed to not allow users to remotely connect to the workstation being configured for local-only access. The System Properties dialog can be found on the control panel of the workstation. (See Figure 4.)

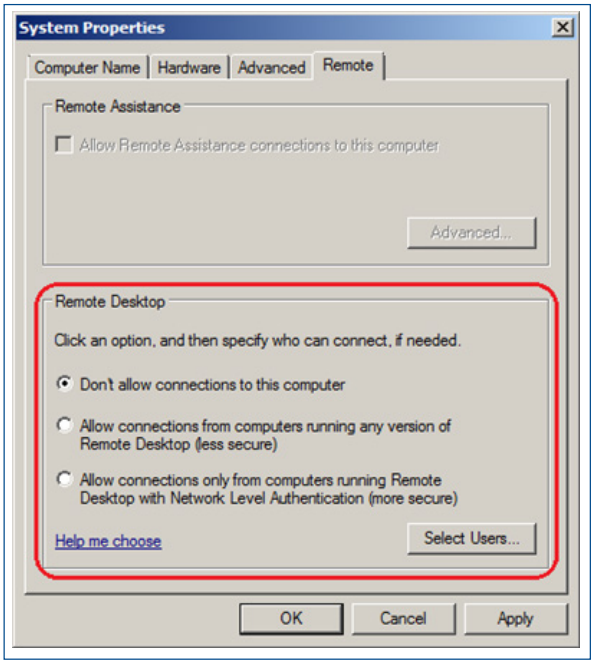


Figure 4 – Remote Desktop settings on Microsoft Windows 7 / Microsoft Windows Server 2008 R2

Secure Remote Access to DeltaV Systems

If Smart Cards are used to also authenticate connections to a DeltaV Remote Desktop Servers, then deploying an intermediate Remote Desktop Gateway server is highly recommended. The Remote Desktop Gateway server will protect the Remote Desktop Server and yet allow Smart Card credentials to be authenticated and forwarded accordingly. (See Figure 5.) Please refer to DeltaV Books OnLine for additional details on how to configure these settings (DeltaV v13.3.1 and higher).

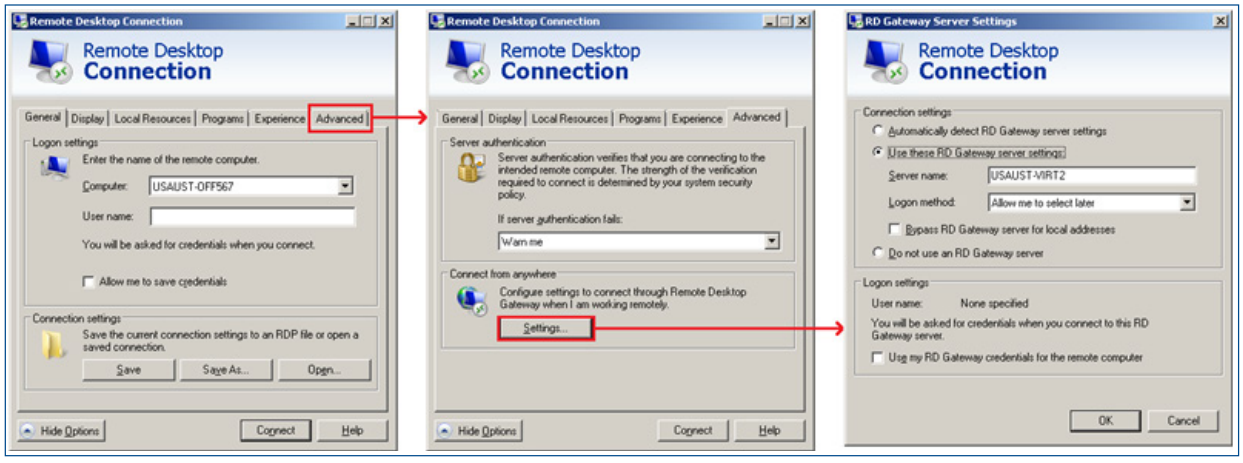


Figure 5 – Remote Desktop settings at the client side to use the Remote Desktop Gateway server

Microsoft Smart Card Enrollment

Smart Card Two-Factor Authentication will work with any hardware compatible with the Microsoft Crypto API Interface. System administrators must run the utilities supplied with the card reader to set up the cards for each user. They must also use the required Microsoft Certificate Authority Server application to enroll users' certificates and embed them on the users' cards either through web enrollment or by using the Microsoft Management Console. (See Figures 6 and 7.)

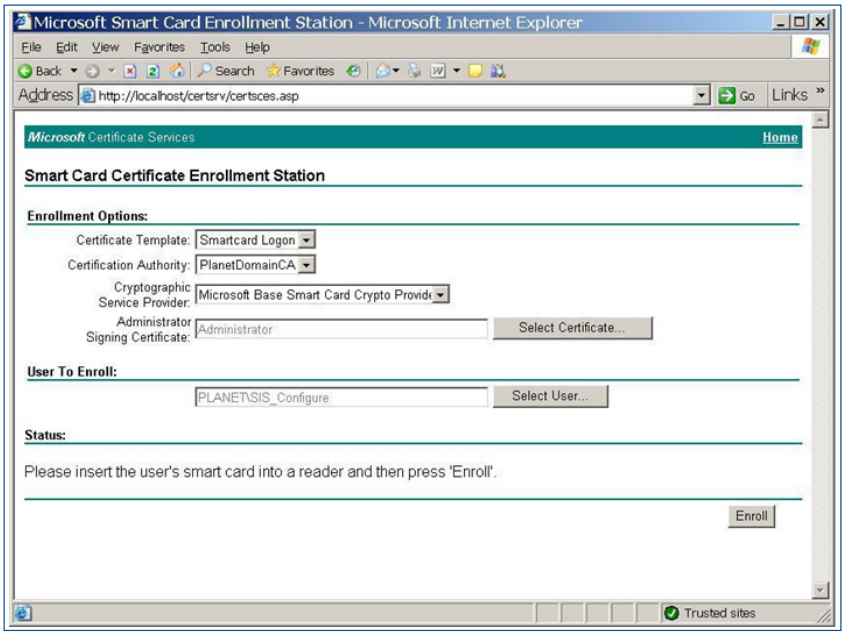


Figure 6 – Certificate web enrollment

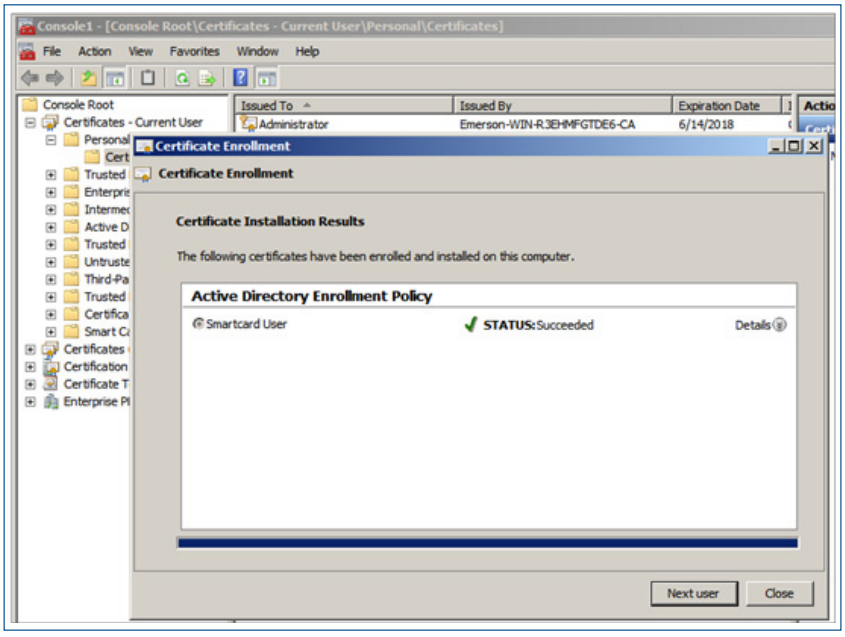


Figure 7 – Certificate enrollment via Microsoft Management Console

Summary

- This security enhancement is supported in DeltaV v9.3 and later.
- Two options are available: card allowed and card required. If the DeltaV card required option is chosen, then it is highly recommended to apply the same option to all workstations and servers within the DeltaV Area Control Network for security reasons.
- The setting is stored in the workstation's registry and will persist through future upgrades of the DeltaV software.
- The Smart Card readers must be compatible with supported O/S according to the DeltaV release where Two-Factor Authentication is being deployed.
- The DeltaV system has been fully tested with Gemalto™ (Safenet™) smart cards and smart card readers.

The DeltaV system uses the utilities supplied with the card reader, which can be obtained directly from the supplier (e.g. Gemalto).

- Smart Card authentication replaces the conventional single factor DeltaV logon process using password, by a two-factor authentication using a physical card and a PIN for DeltaV workstations and servers.

System Requirements

The system requirements to deploy smart card Two-Factor Authentication on DeltaV systems are:

- Windows Active Directory services for the DeltaV software
- A Microsoft Windows Server with Certificate Authority deployed
- Compatible Smart Card readers installed on DeltaV workstations requiring Two-Factor Authentication
- The Windows Group Policy "smartcard required" for interactive logon is not supported on DeltaV workstations and servers.

Support

Smart Card Two-Factor Authentication works only with contact-based smart cards and not biometric devices (e.g. fingerprint readers), nor contactless devices (e.g. tokens, contactless cards, etc.). Any smart card readers that are compatible with the Microsoft Windows O/S supported on any given DeltaV version can be considered.

The Two-Factor Authentication solution is expected to provide an additional layer of protection to your DeltaV DCS to help avoid certain types of undesired actions. The Two-Factor Authentication represents only one portion of an overall DeltaV security solution. Using smart cards does not guarantee that your DeltaV system is secure from cyber-attacks, intrusion attempts, or other undesired actions. Users are solely and completely responsible for their control system security, practices and processes, and for the proper configuration and use of the Two-Factor Authentication solution.

Emerson Process Management
Asia Pacific: 65.6777.8211
Europe, Middle East: 41.41.768.6111
North America, Latin America:
T 1 (800) 833-8314 or
1 (512) 832-3774
www.emersonprocess.com/deltav

DeltaV™

EMERSON™
Process Management