The increasing need for robust data center security has led to the development of high-security features in both hardware and software. One enhanced security measure currently being adopted in many enterprise data centers is two-factor authentication. Two-factor authentication is based on both an object or device (such as a smart card or USB key) and specific knowledge (such as a PIN or password). Standard single-factor authentication, in contrast, is based only on specific knowledge.

The Dell Remote Access Controller 5 (DRAC 5) has implemented a smart card logon feature in firmware version 1.30 as a method for two-factor authentication. Currently, this feature is supported only on Microsoft Windows clients using Microsoft Internet Explorer 6 and later.

Configuring users for smart card logon

Before enabling the smart card logon feature, administrators should first configure local DRAC 5 users or Microsoft Active Directory® directory service users for smart card logon. They can enable local users in the DRAC 5 graphical user interface (GUI) by selecting Remote Access > Configuration > Users, then selecting from the configurable users available.

Microsoft Active Directory configuration for smart card logon in DRAC 5 firmware version 1.30 is the same as in previous firmware versions. Administrators can perform this configuration in the DRAC 5 GUI by selecting Remote Access > Configuration > Active Directory. They should then configure the Domain Name System (DNS) server, upload the Active Directory, and then configure the smart card logon feature.

Figure 1 displays the options available for each user. When enabling a user for smart card logon, administrators should upload the user’s smart card certificate and the trusted Certificate Authority (CA) certificate to the DRAC 5. They can obtain the user certificate by exporting the smart card certificate using the card management software—typically available from the smart card vendor—from the smart card to a Base64-encoded file. They can then upload this file to the DRAC 5 as the user certificate. The trusted CA that issues the smart card user certificates typically also exports the CA certificate to a Base64-encoded file, which administrators can then upload to the DRAC 5. Administrators should configure each user with the username that matches the user principal name in the smart card certificate. For example, for a smart card certificate issued to sampleuser@domain.com, administrators should use “sampleuser” as the username.

For more information on enabling smart card logon with third-party CAs, visit support.microsoft.com/kb/281245.
Directory CA certificate to the DRAC 5, and enable Active Directory logon.

CONFIGURING SMART CARD LOGON IN THE DRAC 5

Administrators can enable smart card logon in the DRAC 5 GUI by selecting Remote Access > Configuration > Smart Card (see Figure 2). If the Configure Smart Card Logon attribute is set to Disabled, the system prompts for a username and password when users attempt to log in through the GUI or through a command-line interface (CLI). If this attribute is set to Enable or to Enable with Remote Racadm, the system prompts for a smart card when users attempt to log in through the GUI. Other interfaces that do not support smart cards are automatically disabled: the Enable setting disables CLI out-of-band interfaces that support only single-factor authentication—such as Telnet, Secure Shell (SSH), serial consoles, remote racadm, and Intelligent Platform Management Interface (IPMI) Over LAN—while the Enable with Remote Racadm setting disables the same set of interfaces but leaves remote racadm enabled. Typically, administrators should use the Enable setting, reserving the Enable with Remote Racadm setting for when a DRAC administrator needs to access the DRAC 5 to run scripts using remote racadm commands.

The other available smart card logon option—Enable CRL check for Smart Card Logon—provides a check box to enable or disable the certificate revocation list (CRL) check for smart card certificates. This optional step, applicable only for smart card users logging in to an Active Directory database, verifies that the DRAC certificate is not listed as revoked in the CRL downloaded from the CRL distribution server. CRL distribution servers are listed in smart card certificates.

USING SMART CARD LOGON IN THE DRAC 5

After administrators have configured smart card logon for local DRAC 5 and Microsoft Active Directory users and enabled the smart card logon feature, the DRAC 5 GUI displays the smart card login page when users attempt to access the DRAC 5 (see Figure 3). If the Microsoft ActiveX® smart card reader plug-in is not present on the user’s client system, the system prompts them to download and install it before continuing. After they have inserted their smart card into the reader and clicked the Login link, the DRAC 5 prompts them for the smart card PIN (see Figure 4).

If the user enters the correct PIN, the DRAC 5 verifies the user’s private key on the smart card, the validity of the digital signature of the certificate, the certification chain from the trusted CA, and the expiration date of the certificate. It also confirms that the user
is enabled in its database; if so, then the user is logged in to
the DRAC 5. If the user is not found or not enabled, the DRAC 5 checks
to see whether the user is enabled for Active Directory login; if so,
the DRAC 5 attempts to log the user in through Active Directory,
and simultaneously attempts to download and check the CRL for
the user certificate, if that option is enabled. The Active Directory
login fails if the certificate is listed as revoked in the CRL or if the
CRL cannot be downloaded. Finally, the DRAC 5 prompts the user
for the Active Directory password for the username retrieved from
the smart card (see Figure 5).

**Troubleshooting Smart Card Logon in the DRAC 5**

If problems occur with smart card logon, administrators can take
several steps to help resolve them depending on the specific problem:

- **Microsoft ActiveX plug-in cannot detect smart card reader:**
  Administrators should first verify that the smart card is sup-
  ported by the Microsoft Windows OS.2 Windows supports a
  limited number of smart card cryptographic service providers
  (CSPs) out of the box; unsupported smart cards require
  administrators to install the appropriate CSPs provided by the
  smart card vendor. Administrators can check whether smart
card CSPs are present on a particular client by inserting the
  smart card in the reader at the Windows login screen (accessed
  by pressing Ctrl+Alt+Del) and seeing whether Windows
detects the smart card and prompts for the PIN. They can also
try to log in to Windows using the smart card.

- **Smart card rejects correct PIN:** Administrators should check
  whether the smart card has been locked following multiple
  login attempts with an incorrect PIN. If this is the case, they
  should check with the organization’s smart card issuer to
  obtain a new card.

- **Local DRAC 5 user cannot log in:** Administrators should
  check whether the username and user certificates uploaded
to the DRAC 5 have expired. The DRAC 5 trace logs may also
  provide important messages regarding the errors, although
  these messages are sometimes intentionally ambiguous for
  security reasons.

- **Microsoft Active Directory user cannot log in:** Administrators
  should try logging in to the DRAC 5 after disabling smart card
  logon. The DRAC 5 trace logs may also provide important
  messages on CRL failures.

If necessary during troubleshooting, administrators can dis-
able the smart card logon through local racadm using the fol-
lowing command:

```
racadm config -g cfgActiveDirectory -o
cfgADSmartCardLogonEnable 0
```

They can also use the option ROM, which can be accessed
during the server power-on self-test by pressing Ctrl+E, to con-
figure smart card logon (see Figure 6).

**Enhancing DRAC 5 Security**

The smart card logon feature in DRAC 5 firmware version 1.30
is designed to support secure two-factor authentication when
logging in to the DRAC. By enabling this feature, administrators
help increase security in their environment.

**Sriranjan Bose** works with the Enterprise Embedded Software
Group at the Dell Bangalore Development Center. Previously, he
was an engineer analyst with the Enterprise Software Product
Test Group.

**Abhay Salunke** is a senior software developer in the Remote
Access Firmware Group at Dell. He is the technical lead for several
DRAC projects and has contributed to various Dell OpenManage™
software development projects.

---

2 A list of supported smart cards is available at technet2.microsoft.com/windowsserver/en/library/6faa74b1-4e2-45f9-8e13-3bbaa1a43411d3.mspx.