Delinea

Server Suite

Smart Card Configuration Guide

Version: 2023.x

Publication Date: 5/16/2024

Server Suite Smart Card Configuration Guide

Version: 2023.x, Publication Date: 5/16/2024

Table of Contents

Smart Card for Red Hat Linux

This document explains how to set up smart card authentication for logging on to Red Hat Linux computers.

Why and How to Use a Smart Card to Log On

Smart cards provide an enhanced level of security for Red Hat Linux computers when users log on to Active Directory domains. If you use a smart card to log on, authentication requires a valid and trusted root certificate or intermediate root certificate that can be validated by a known and trusted certification authority (CA).

Because smart cards rely on a public-private key infrastructure (PKI) to sign and encrypt certificates and validate that the certificates were issued by a trusted certification authority and have not expired or been revoked, authentication using a smart card is more secure than a user name and password.

Configuring a smart card for use on a Red Hat Linux computer that is running the Delinea Agent requires that you have already set up a smart card for use in a Windows domain. You do not need to add any smart card infrastructure to the Linux computer, other than a smart card reader and a provisioned smart card.

In a Windows environment, a smart card may be set up either for a single user account or for multiple user accounts. For example, an individual contributor might have access to a single Active Directory account that he uses for all his work. In this case, the card is set up for a single user and the card is linked directly to a UPN. When a user inserts the card to log on, the smart card system looks for the UPN in Active Directory and prompts for a PIN.

Windows 2008 also provides a name-mapping feature that enables configuring a smart card with multiple user accounts. For example, a user might want to log in with a regular account to check mail or perform routine tasks, but log in with an administrator's account to perform privileged tasks. To set up a card for multiple users, an administrator maps a certificate to each user account on the card. When a user inserts the card to log on, the smart card system prompts the user to select which account to use, and prompts for the card's PIN.

If you have set up smart card login for Windows clients in a domain, you can use Access Manager to configure smart card login for Red Hat Linux clients joined to the same domain. If you have provisioned a smart card for use on a Windows computer – either for a single user or multiple users – once you configure smart card support for a Linux computer, you can use the same smart card to log in to a Red Hat Linux computer.

> Configuring smart card support in Access Manager is nearly the same for a single-user or multi-user card with the exception that for multi-user cards, you must set an extra configuration parameter as explained in Enabling Support for Multi-User Smart Cards.

Setting up a single user smart card login for Windows computers requires either:

- Microsoft enterprise root certification authority; see the Microsoft TechNet article: Install an enterprise root certification authority.
- A third party certification authority – see the Microsoft KB article: Guidelines for enabling smart card logon with third-party certification authorities.

Setting up a multi-user smart card login for windows requires mapping the certificate on the card to the users who the card is associated with. See the following Microsoft Technet Blog post: Mapping One Smart Card to Multiple Accounts for more information on how to do this.

Configuring Smart Card Authentication

You configure Red Hat Linux computers for smart card authentication primarily through group policy settings. Enabling support for smart cards requires that you set a single policy (“Enable smart card support”). Supporting the use of multi-user smart cards requires that you set a configuration parameter on each Red Hat computer. In addition, Server Suite provides several group policies to control how smart card authentication works after you enable it.

Complete the procedures in the following sections to configure smart card authentication for Red Hat Linux computers:

- Enabling smart card support in which you enable smart card authentication for Active Directory users. This is the only procedure you need to complete to enable smart card authentication. The other procedures allow you to configure different aspects of smart card authentication, such as locking the screen if the smart card is removed, or preventing users from logging in without a smart card.
- Enabling support for multi-user smart cards in which you set the smart card.name.mapping configuration parameter to enable the use of smart cards provisioned with multiple users on a particular computer.
- Enforcing smart card authentication in which you prevent users from logging in with a user name and password on Red Hat Linux computers that have smart card authentication enabled. You can require all users on a computer to use a smart card for logging in or require specific users to use a smart card.
- Configuring certificate validation in which you specify how to use a Certificate Revocation List (CRL) to check the status of certificates stored on a revocation server
- Locking the screen if a smart card is removed in which you require that the computer’s screen is locked when a smart card is removed.
- Enabling a certificate without extended key usage in which you enable a Windows group policy setting to allow using certificates without the EKU attribute for smart-card log in.
- Configuring applications for smart card access in which you configure applications such as Firefox and Thunderbird that require smart card authentication to gain access to sensitive sites and data.

Before Configuring Smart Card Authentication

To use a smart card to log on to a Red Hat Linux, CentOS, Debian, or Ubuntu computer, verify that the computers meet these requirements:

- Supported operating systems:
  - Red Hat Linux (amd64) version 5.6 or later
  - CentOS (amd64) version 5.6 or later
  - Ubuntu 18.04.x LTS, 20.04.x LTS, 21.04, 22.04.x LTS and 22.10 (amd64)
  - Debian 9.x and 10.x or later(amd64)
  - Oracle Linux 8 or later (amd64)
  - Rocky Linux (amd64)

- AlmaLinux (amd64)

> For Debian and Ubuntu systems, be sure to have the `opensc-pkcs11`, `pcscd`, and `libnss3-tools` packages installed.

- Are running the GNOME desktop. The agent does not support use of a smart card with the KDE desktop.
- If a system is running RedHat Linux or CentOS 8.0 or later, the system needs Server Suite Agent for *NIX version 5.7.0 or later.
- If a system is running Debian or Ubuntu, the system needs Server Suite Agent for *NIX version 5.8.0 or later.
- Are joined to the Windows domain.
- Have a supported smart card reader attached.

Other prerequisites for enabling smart card support differ depending on whether you have configured a single-user or multi-user smart card.

For a single-user card, before enabling smart card support, make sure you do the following:

- Provision a smart card with an implicit or explicit certificate-to-user mapping.
  - Currently, Server Suite Agent for *NIX supports Common Access Card (CAC) and Personal Identify Verification (PIV) cards with both CAC and PIV profiles (CACNG) and Alternative Logon Token (ALT) smart cards.
  - Server Suite Agent for *NIX supports implicit certificate-to-user mapping where the certificate's Principal Name in the Subject Alternative Name (SAN) matches the user's userPrincipalName (UPN) or Kerberos v5 principal name in Active Directory (AD).
  - Alternatively, explicit mapping by way of the user's `altSecurityIdentities` AD attribute is also supported.

> Mapping one certificate to multiple users is not supported.

- Verify that the Active Directory user is successfully mapped by running the `sctool --dump` command.

For a multi-user card, before enabling smart card support, make sure you have the following in place:

- A Windows Server 2008, or later, domain controller for authentication.
- The card is not configured with a UPN. If a card with a UPN is inserted, the computer prompts for a PIN rather than prompting for a user name and password.
- An administrator has added the certificate on the card to the name mapping for the users the card is associated to. See the following Microsoft Technet Blog postMapping One Smart Card to Multiple Accounts for more information on how to do this.

For either type of card, verify that the public key infrastructure to support smart card login is operational on the Windows computer running Active Directory and Access Manager. If the user is able to log in to a Windows computer with a smart card, and you have a card reader and a fully-provisioned card for the Linux computer, the user should be able to log in to the Linux computer once you configure it for smart card support.

Although the Linux computer has its own infrastructure for enabling and managing smart card authentication, the Server Suite Agent for *NIX and smart card utility (sctool) enable authentication through Active Directory. After you

enable smart card support through the Server Suite Agent, the Red Hat smart card configuration options have no effect.

Enabling Smart Card Support

Smart card authentication requires configuration changes to certain Red Hat or CentOS Linux files, depending on the version of Red Hat Linux or CentOS you are using.

For example, if you are using Red Hat Linux 5.6 or 6.0, the files affected may include the following:

- `/etc/pam.d/gdm`
- `/etc/pam.d/gnome-screensaver`
- `/etc/pam.d/password-auth`
- `/etc/pam.d/smartcard-auth`

Smart card authentication also requires configuration changes to certain system Coolkey symbolic links such as the following:

- `/usr/lib(64)/libckyapplet.so.1.0.0`
- `/usr/lib(64)/pkcs11/libcoolkeypk11.so`

After you enable smart card authentication, the agent makes the required changes and creates backup copies of the affected files.

The smart card components on the Linux computer are configured by default to use the Delinea Coolkey PKCS #11 module for authentication. Although this is the optimal configuration, if your smart cards are not supported by Coolkey, Delinea allows you to specify a different PKCS #11 module to use for authentication. Delinea does not supply PKCS #11 modules other than the default Coolkey module. If you need to use a third-party module, you must install it yourself.

Some PKCS #11 modules may not work seamlessly with the GDM environment. For example, some card events, such as locking the screen upon card removal, may not work.

To configure a different module, do one of the following:

- If you are enabling smart card support with group policy, you can specify an alternate PKCS #11 module when you enable the group policy; see the procedure: To enable smart card support by using group policy.
- If you are manually enabling smart card support by running `sctool`, you can set a configuration parameter on each Linux computer to specify the module to use; see the procedure: To manually enable smart card and specify a different PKCS #11 module.

Steps

If you are running Red Hat Linux 6.0, you must install some support packages before enabling smart card support; see To install required packages on Red Hat Linux 6.0.

You can enable smart card authentication by either of the following methods:

- Use the “Enable smart card support” group policy, which enables smart card support on all computers to which the Group Policy object applies. Note that configuration changes do not take place until the next group policy

update or when you run `adgpupdate` on the Linux computers.

- Run the sctool -enable utility on each computer that you want to enable for smart card support.

To install required packages on Red Hat Linux 6.0

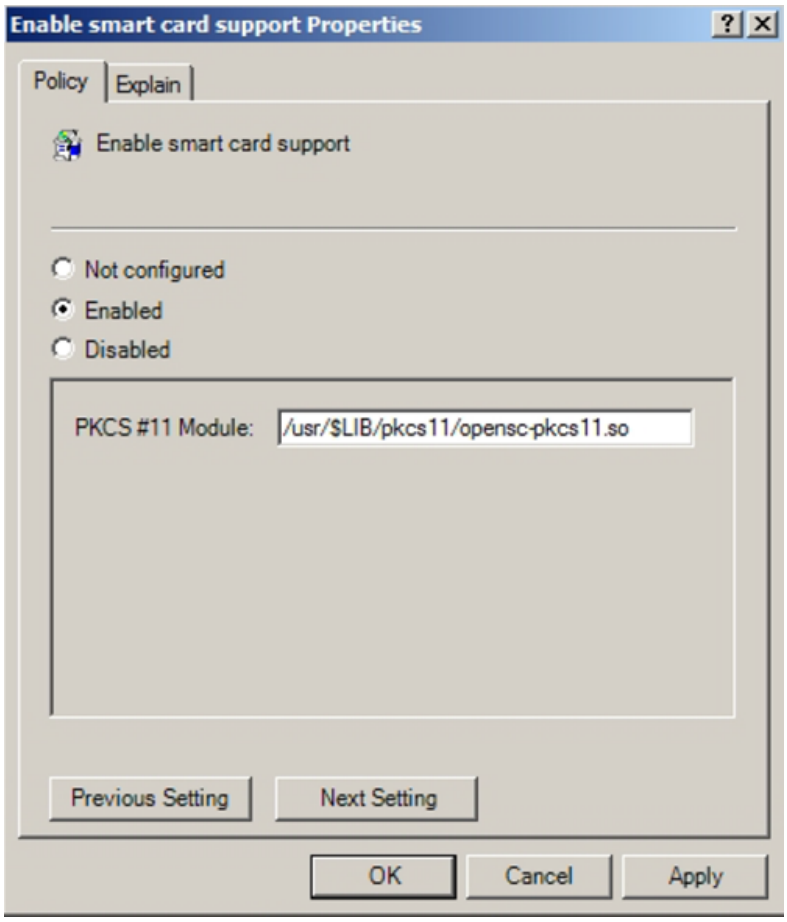
1. Log on to a Red Hat computer with root privilege and open a terminal window.
2. Run the following command:

   ```
   [root]#yum groupinstall "Smart card support"
   ```

To Enable Smart Card Support Using Group Policy

1. On a Windows computer, open Group Policy Management to create or select a Group Policy object that is linked to a site, domain, or organizational unit that includes Red Hat Linux computers; right-click the Group Policy object, then select **Edit**.
2. In the Group Policy Management Editor, expand **Computer Configuration** > **Policies** > **Delinea Settings** > **Linux Settings**, click **Security**, then double-click **Enable smart card support**.
3. Select **Enabled**, then click **OK** to save the policy setting, or go to the next step to change the PKCS #11 module used for authentication.

   This group policy modifies Red Hat Enterprise Linux configuration files to look for a smart card user's credentials in Active Directory and verify the identity of the user with the smart card certificate.
4. Optionally, to specify a PKCS #11 module other than the Delinea default module, type the complete path to the module in **PKCS #11 Module**:



> Your smart card environment performs optimally when configured to use the default Coolkey module. You should specify a different module only if your smart cards are not supported by Coolkey. Otherwise, skip this step and click **OK** to save the group policy setting.

This field supports the use of the $LIB environment variable in the path to allow a single group policy to work for 32-bit and 64-bit systems. At run time on 32-bit systems$LIBresolves tolib, while on 64-bit systems it resolves to lib64.

For example, the following path specifies the OpenSC PKCS #11 module:

```
/usr/$LIB/pkcs11/opensc-pkcs11.so
```

5. To apply the group policy immediately to any computer you must restart the computer or run the adgpupdate command on it.

   Otherwise, all affected computers will be updated automatically at the next group policy update interval. After computers are restarted or receive the policy update, they are ready for smart card use.

To Manually Enable Smart Card Support Running sctool

1. Log on to a Red Hat computer with root privilege and open a terminal window.
2. Run the sctool utility with the --enable option:

   ```
   [root]$ sctool --enable
   ```
3. Repeat steps 1 and 2 for each computer on which to enable smart card authentication.

To Manually Enable Smart Card and Specify a Different PKCS #11 Module

1. Open the Delinea configuration file with a text editor, find the rhel.smartcard.pkcs11.module parameter, and set its value to the complete path for your PKCS #11 module.

   Be certain to remove the comment for the parameter.

   For example, the following parameter value sets PKCS #11 to the OpenSC module:

   ```
   [user]$ vi /etc/centrifydc/centrifydc.conf
   ```

   ...

   rhel.smartcard.pkcs11.module: /usr/$LIB/pkcs11/opensc-pkcs11.so

   This parameter supports the use of the $LIB environment variable in the path to allow a single path specification to work for 32-bit and 64-bit systems. At run time on 32-bit systems $LIB resolves to lib, while on 64-bit systems it resolves to lib64.
2. Save and close the file.
3. Enable, or re-enable smart card support by running the following sctool commands as root:

   ```
   [root]$ sctool --disable
   ```

   [root]$ sctool --enable
4. Refresh the GNOME environment by running the following command as root:

   ```
   [root]$ /usr/sbin/gdm-safe-restart
   ```

Next Steps

After you enable smart card support, the computer is ready for smart card authentication. You can attach a smart card reader and log in with a valid card and matching Active Directory user.

The next step is to configure one or more of the following smart card authentication options if you wish:

- Enabling support for multi-user smart card which sets the smartcard.name.mapping configuration parameter to enable the use of smart cards provisioned with multiple users on a particular computer.
- Enforcing smart card authentication which prevents users from logging on with just a user name and password.
- Configuring certificate validation which specifies how certificates are validated.
- Locking the screen if a smart card is removed which locks the screen when a smart card is removed to provide enhanced security.

If you have no other options to configure, you can go directly to Verifying smart card authentication to confirm that you can log on to one of the Linux computers that you have configured for smart card authentication.

Enabling Support for Multi-User Smart Cards

If you plan to use multi-user smart cards on a Red Hat Linux computer in your domain, you must set the `smartcard.name.mapping` parameter to true in the Delinea configuration file for that computer by completing the following the procedure. If your environment exclusively uses single-user smart cards, you can skip this section.

> Setting the configuration parameter with this procedure has no effect on single-user smart cards. There is no conflict with using single-user and multi-user on the same computer. However, if a Red Hat Linux computer is accessed through a multi-user card, you must set the configuration parameter by using this procedure.

To enable support for multi-user smart cards

1. On the Red Hat Linux computer, open the Delinea configuration file in a text editor, `/etc/centrifydc/centrifydc.conf`, with a text editor.
2. Type the following:

   ```
   smartcard.name.mapping: true
   ```

   By default, this parameter is set to false and the configuration file should have a commented line showing this setting. So, alternately, you can find this parameter in the file, remove the comment, and change the value to true.
3. Save and close the file.

Enforcing Smart Card Authentication

By default, enabling smart card support does not force all users to log on using a smart card. If you want to require all Active Directory users to authenticate by using a smart card, you have the option to configure a computer group policy. If you want to require only specific Active Directory users to authenticate by using a smart card, you can configure their user account properties to require a smart card for authentication.

You can enable the “Require smart card login” group policy to ensure that all Active Directory users logging on to a computer must insert a smart card for authentication. If you enable this policy, Active Directory users who forget their smart card will be unable to log on to their computers. However, you add exceptions to this group policy to allow users who forget their smart card to log on using their user name and password on the computers where the policy with exceptions is applied.

> If you use this approach to enforce smart card login for all users, be certain that all users have their accounts set with the “Password never expires” option. If a user attempts to log on with a smart card but the password for the account has expired, the smart card login fails with an error message about changing the password. If you use the account option to require smart card for specific users, you can ignore password expiration.

Enforcing smart card authentication applies to all forms of log on, including GUI login, SSH, telnet, and so on. However, it is enforced for Active Directory users only. If a computer is configured with one or more local accounts, those accounts are still able to log on even if you set the group policy to require smart card authentication.

Steps

To require smart card login, complete one of these procedures

- To require smart card login for all users on a computer
- To require smart card login for a specific user

To require smart card login for all users on a computer

1. On a Windows computer, open Group Policy Management and select the Group Policy object where you enabled smart card support for Red Hat Linux computers; right-click the Group Policy object, then click **Edit**.
2. In the Group Policy Management Editor, expand **Computer Configuration** > **Policies** > **Centrify Settings** > **Linux Settings**, click **Security**, then double-click **Require smart card login**.
3. Select **Enabled**.

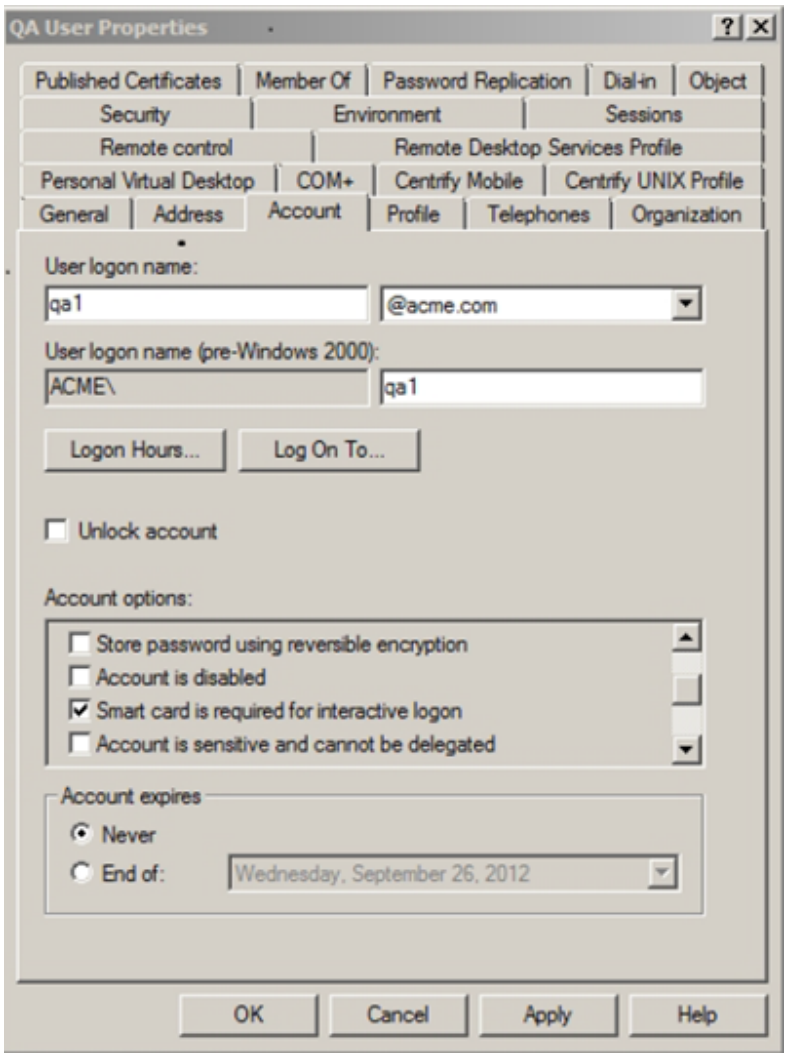
   Click **Add** if you want to add exceptions to this group policy now, then click Browse to search for and select the Active Directory group allowed to log on using a user name and password if they forget their smart card. If you only want to configure exceptions when they are needed, click **OK** to enable the group policy without exceptions.
4. To apply the group policy immediately to any computer, you must restart the computer or run the adgpupdate command on it.

   Otherwise, all affected computers will be updated automatically at the next group policy update interval.

To require smart card login for a specific user

1. On a Windows computer, open the Access Manager console or Active Directory Users and Computers.
2. Select the user.

   For example, in the Administrator's Console, open *domainName* __> **Zones** >** *zoneName* **> **UNIX Data** > **Users**.
3. Right-click the user's name and select **AD Properties**.
4. In the User Properties window for the user, click the **Account** tab.
5. In "Account options", scroll until **Smart card is required for interactive logon** is visible, then select it.



6. Click **OK**.

Configuring Certificate Validation

You can use the **Certificate validation method** group policy to configure how certificates are validated or rejected by using a Certificate Revocation List (CRL) stored on a revocation server.

To Configure How Certificates are Validated

1. On a Windows computer, open Group Policy Management and select the Group Policy object where you enabled smart card support for Red Hat Linux computers; right-click the Group Policy object, then click **Edit**.
2. In the Group Policy Management Editor, expand **Computer Configuration** > **Policies** > **Centrify Settings** > **Linux Settings**, click **Security**, then double-click **Certificate validation method**.
3. Select **Enabled**.
4. Choose one of the following options from **Certificate Revocation List**:

- **Off:** To disable certificate validation.

  If you select this setting, no revocation checking is performed.

- **Best attempt:** To check that certificates are not rejected as invalid, untrusted, or revoked by the certificate revocation list (CRL).

  This setting is appropriate for most organizations.

- **Require if cert indicates:** To check whether there is a successful connection to the revocation server.

  If a URL to the revocation server is provided in the certificate, this setting requires a successful connection to a revocation server, and checks that certificates are not rejected as invalid, untrusted, or revoked by the CRL. You should only use this setting in a tightly controlled environment that guarantees the presence of a CRL server. If a CRL server is not available, certificate validation may prevent furthering processing of an authentication request.

- **Require for all certs:** To require successful validation of all certificates.

  You should only use this setting in a tightly controlled environment that guarantees the presence of a CRL server. If a CRL server is not available, certificate validation may prevent furthering processing of an authentication request.

5. Click **OK** to save the policy settings.
6. To apply the group policy immediately to any computer, restart the computer or run the `adgpupdate` command on it.

   Otherwise, all affected computers will be updated automatically at the next group policy update interval.

Locking Screen if Smart Card is Removed

Depending on what you consider best practices for using a smart card, you may want the screen to lock whenever a user removes the smart card. If you want to lock the screen when a smart card is removed, you can do so by enabling the **Removing a smart card locks screen** user group policy.

To lock the smart card screen when a smart card is removed

1. On a Windows computer, open Group Policy Management and select the Group Policy object where you enabled smart card support for Red Hat Linux computers; right-click the Group Policy object, then click **Edit**.
2. In the Group Policy Management Editor, expand **Computer Configuration** > **Policies** > **Centrify Settings** > **Linux Settings**, click **Security**, then double-click **Lock Smart Card screen for RHEL**.
3. Select **Enabled**, then click **OK**.

   Note: Policies are turned off by default on Linux systems but can be turned on with a group policy setting. To ensure that the “Removing a smart card locks screen” policy takes effect, verify that the following computer policy is enabled by completing the following two steps.

4. Expand **Computer Configuration** > **Centrify Settings** > **DirectControl Settings**, click **Group Policy Settings**, then double-click **Enable user group policy**.
5. Verify that **Enabled** is selected, and if not, select it, then click **OK**.
6. To apply the group policy “Lock Smart Card screen for RHEL” immediately to any computer you must restart the computer or run the `adgpupdate` command on it.

Otherwise, all affected computers will be updated automatically at the next group policy update interval. After computers are restarted or receive the policy update, the screen is locked if a smart card is removed.

Enabling a Certificate Without Extended Key Usage

Normally, smart card use requires certificates that contain the extended key usage (EKU) attribute. However, Windows provides a group policy that allows the use of certificates that do not have the EKU attribute.

> This group policy is implemented as an administrative template (.adm file), not as an xml file, as are the Delinea group policies.

To use certificates without the EKU attribute with smart cards:

1. Open the group policy editor and edit the GPO that contains the Linux computers enabled for smart-card login.
2. Open **Computer Configuration > Policies > Administrative Templates > Windows Components > Smart Card** and double-click **Allow certificates with no extended key usage certificate attribute**.
3. Click **Enabled** and click **OK**.

   When you enable this policy, it sets the `smartcard.allow.noeku` parameter to true in the Delinea configuration file. Certificates with the following attributes can also be used to log on with a smart card:

   - Certificates with no EKU
   - Certificates with an All Purpose EKU
   - Certificates with a Client Authentication EKU
4. In a Terminal window, run the `sctool` command as root with the `-E (--no-eku)` parameter to re-enable smart card support. You must use either the `-a (--altpkinit)` or `-k (--pkinit)` parameter with the `-E` option; for example:

   ```
   sctool -E -k jsmart@acme.com
   ```

Configuring Applications for Smart Card Access

Many applications, including Firefox and Thunderbird, that require smart card access to sensitive sites or data, create their own NSS database for the user. To give these applications access to the certificates and control revocation lists (CRL) used by the agent for log on, you enable the group policy “Specify applications to import system NSSDB”, which synchronizes the system NSSDB file on a computer with each application’s NSSDB file.

Each application, such as Firefox, creates a profile file (profile.ini) that specifies the location for its certificates and CRLs. With the “Specify applications to import system NSSDB” policy, you specify the location of the profile file for an application. A Delinea mapper file parses the profile file to determine the location of the application’s certificates and CRLs and copies certificates and CRLs to this location.

Steps

If the computers you manage use applications such as Firefox that require smart card access to sensitive sites or data, configure NSS database synchronization to ensure that these applications have access to current certificates and control revocation lists.

To configure NSS database synchronization

1. On a Windows computer, open Group Policy Management and select the Group Policy object where you enabled smart card support for Red Hat Linux computers; right-click the Group Policy object, then select **Edit**.
2. In the Group Policy Management Editor, expand **User Configuration** > **Policies** > **Centrify Settings** > **Linux Settings**, click **Security**, then double-click **Specify applications to import system NSSDB**.
3. Select **Enabled**, then click **Add**.
4. In **Application**, specify the application directory in which to import the system NSS database.

   For each application enter the location of its profiles.ini file. Specify the entry in relation to the home directory of the user by starting the path with ~/. For example, the following entry specifies the default location of the Firefox profiles.ini file

   `~/.mozilla/firefox.`
5. Click **Add** to add as many application directories as necessary, then click **OK** to save the settings.

   Note: User policies are turned off by default on Linux systems but can be turned on with a group policy setting. To ensure that the “Specify applications to import system NSSDB” policy takes effect, verify that the following computer policy is enabled:
6. Expand **Computer Configuration** > **Centrify Settings** > **DirectControl Settings**, click **Group Policy Settings**, then double-click **Enable user group policy**.
7. Verify that **Enabled** is selected, and if not, select it, then click **OK**.
8. To apply the group policy immediately to any computer, restart the computer or run the `adgpupdate` command on it.

   Otherwise, all affected computers will be updated automatically at the next group policy update interval. After computers are restarted or receive the policy update, the screen is locked if a smart card is removed.

Configuring Citrix VDA Smart Card Authentication

You can integrate Delinea Agent for *NIX with the Citrix Virtual Delivery Agent (VDA) for Active Directory user authentication. This integration helps users log in to remote Red Hat Linux (RHEL) virtual desktop sessions with a smart card connected to the client device.

The Delinea Authentication Service supports pass-through authentication if the Citrix requirements are met. For details, see https://docs.citrix.com/en-us/linux-virtual-delivery-agent/current-release/system-requirements.html.

Be sure that you have set up smart card authentication already on Windows systems in your domain before continuing.

To configure Citrix VDA smart card authentication:

1. Install the Citrix Linux VDA.

   For details, see the Citrix documentation: https://docs.citrix.com/en-us/linux-virtual-delivery-agent/current-release/installation-overview.html.

   For example, you might run a command that looks like the following:

   ```
   sudo yum -y localinstall XenDesktopVDA-19.9.0.3-1.el7_x.x86_64.rpm
   ```

2. According to the Citrix VDA documentation, install the necessary software and perform the required system integrations.

   NTP isn't required to be configured in an Active Directory environment, but Citrix Linux VDA does require certain software, such as PostgreSQL and openJDK. For details, see https://docs.citrix.com/en-us/linux-virtual-delivery-agent/current-release/configuration.html.

3. Install Delinea Agent for *NIX version 19.9 or later and join the computer to the domain.

   For details, see the **Planning and Deployment Guide**.

4. To configure the agent integrations with the Citrix Linux VDA, add the following setting to the centrifydc.conf file:

   ```
   smartcard.login.service.accounts: ctxsrvr
   ```

   The Citrix smart card login service runs as the `ctxsrvr` account. This parameter allows you to specify a list of non-root user accounts that use the smart card login services.

5. Configure the Citrix Linux Virtual Delivery Agent (VDA).

   For details, see the Citrix documentation: https://docs.citrix.com/en-us/linux-virtual-delivery-agent/current-release/configuration.html and https://docs.citrix.com/en-us/linux-virtual-delivery-agent/current-release/installation-overview/redhat.html.

   Below is an example of running ctxsetup.sh in interactive mode; be sure to adjust as needed for your environment.

```
$ sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
```

Welcome to the Citrix Linux VDA setup script. This script will guide you through the

configuration of the Linux VDA system services. You can re-run this script at

any time to reconfigure the system.

Gathering information...

Checking CTX_XDL_DOTNET_RUNTIME_PATH... Value not set.

Dotnet Core runtime environment is needed to run Linux VDA.

Linux VDA will install it to /opt/dotnet by default.

If required, please specify an absolute path in valid format here (e.g., /the/path). [\<none\>]:

Checking CTX_XDL_SUPPORT_DDC_AS_CNAME... Value not set.

The Virtual Delivery Agent supports specifying a Delivery Controller name using a DNS CNAME record.

Do you want to enable support for DNS CNAME records? (y/n) [n]: y

Checking CTX_XDL_DDC_LIST... Value not set.

The Virtual Delivery Agent requires a space-separated list of Delivery Controller Fully Qualified Domain Names

(FQDNs) to use for registering with a Delivery Controller. Please provide the FQDN of at least one Delivery

Controller: CS.CITRIX.TEST

Checking CTX_XDL_VDA_PORT... Value not set.

The Virtual Delivery Agent by default communicates with Delivery Controllers using TCP/IP port 80.

Please provide the TCP/IP port the Virtual Delivery Agent service (ctxvda) should use to communicate with a

Delivery Controller [80]:

Checking CTX_XDL_REGISTER_SERVICE... Value not set.

The Linux VDA services support starting during boot.

Do you want to register these services to start on boot? (y/n) [y]:

Checking CTX_XDL_ADD_FIREWALL_RULES... Value not set.

The Linux VDA services require incoming network connections to be allowed through

the system firewall. Do you want to automatically open the required ports (by default ports 80, 1494, 2598, 8008 and 6001\~6099) in the

system firewall for the Linux VDA? (y/n) [y]:

Checking CTX_XDL_AD_INTEGRATION... Value not set.

The Virtual Delivery Agent requires Kerberos configuration settings to authenticate with Delivery Controllers. The

Kerberos configuration is determined from the installed and configured Active Directory integration tool on this system. Please select the Active Directory integration tool configured on this system:

1: Winbind

2: Quest

3: Centrify 4: SSSD

5: PBIS

Select one of the above options (1-5) [1]: 3

Checking CTX_XDL_HDX_3D_PRO... Value not set.

Linux VDA supports HDX 3D Pro, a set of graphics acceleration technologies designed to optimize the virtualization of rich graphics applications. HDX 3D Pro requires a compatible NVIDIA Grid graphics card to be installed. If HDX 3D Pro is selected the Virtual Delivery Agent will be configured for VDI desktops (single-session)

mode. Do you want to enable HDX 3D Pro? (y/n) [n]:

Checking CTX_XDL_VDI_MODE... Value not set.

Linux VDA supports delivery of hosted shared desktops (multi-session) or VDI desktops (single-session).

Do you want to enable VDI desktops (single session) mode? (y/n) [n]: y

Checking CTX_XDL_SITE_NAME... Value not set.

The Virtual Delivery Agent discovers LDAP servers using DNS, querying for LDAP service records. To limit the DNS

search results to a local site, a DNS site name may be specified.

If required, please specify a local DNS site name. [\<none\>]:

Checking CTX_XDL_LDAP_LIST... Value not set.

The Virtual Delivery Agent by default queries DNS to discover LDAP servers, however if DNS is unable to provide

LDAP service records, you may provide a space-separated list of LDAP Fully Qualified Domain Names (FQDNs) with

LDAP port (e.g. ad1.mycompany.com:389).

If required, please provide the FQDN:port of at least one LDAP server. [\<none\>]:

Checking CTX_XDL_SEARCH_BASE... Value not set.

The Virtual Delivery Agent by default queries LDAP using a search base set to the root of the Active Directory

Domain (e.g. DC=mycompany,DC=com), however to improve search performance, a search base may be specified

(e.g. OU=VDI,DC=mycompany,DC=com).

If required, please provide an LDAP search base. [\<none\>]:

Checking CTX_XDL_FAS_LIST... Value not set.

The Federated Authentication Service (FAS) servers are configured through AD Group Policy. But because

the Linux VDA does not support AD Group Policy, you can provide a semicolon-separated list of FAS servers instead.

Caution 1: The sequence must be the same as configured in AD Group Policy.

Caution 2: If any server address is removed, you must fill its blank with the '\<none\>' string and keep the index of server addresses without any changes.

If required, please specify the list of FAS servers (e.g., fasserver.company.com). [\<none\>]:

Checking CTX_XDL_START_SERVICE... Value not set.

The Linux VDA services may be started after configuration is complete.

Do you want to start these services once configuration is complete? (y/n) [y]:

Configuring Citrix Linux VDA ...

Configuration complete.

6. In Citrix Virtual Apps or Citrix Virtual Desktops, create the machine catalog and delivery group.

   For details, see https://docs.citrix.com/en-us/linux-virtual-delivery-agent/current-release/installation-overview/redhat.html#step-8-create-the-machine-catalog-in-citrix-virtual-apps-or-citrix-virtual-desktops.
7. (Optional) Enable the group policy entitled "Enable smart card support."
8. Verify that the smart card login is enabled on the Linux computer:

   ```
   $ sudo sctool -s
   ```

   Delinea Smart Card support is enabled.

   If you have not enabled the group policy enabled "Enable smart card support", you may need to run the following command to enable smart card login:

   ```
   $ sctool -e
   ```

   For details about this group policy, see the **Smart Card Configuration Guide**.
9. Reboot the Linux computer.
10. In Citrix StoreFront, enable smart card authentication.

    For details, see https://docs.citrix.com/en-us/storefront/current-release/configure-authentication-and-delegation/configure-authentication-service.html.

Verifying Smart Card Authentication

After you enable smart card support, you should verify that a user is able to authenticate with a smart card on a Red Hat Linux computer.

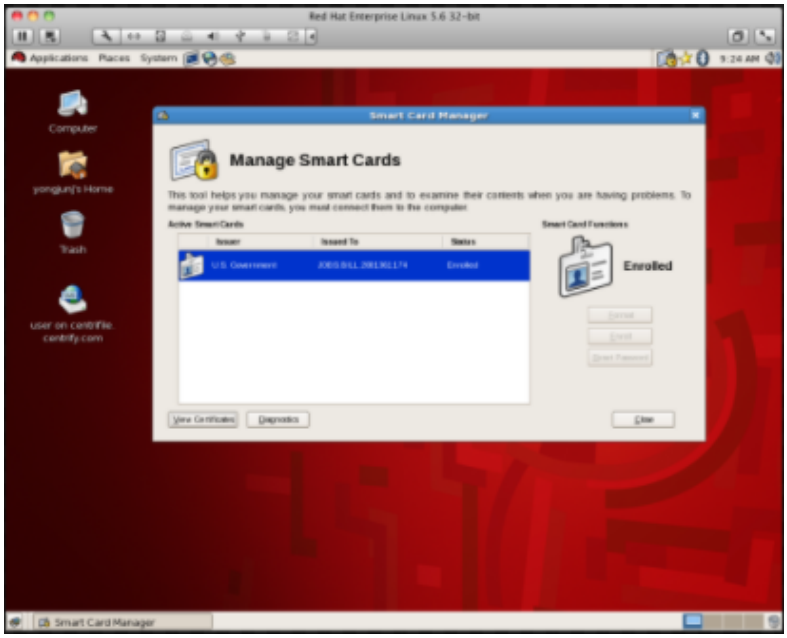
To verify smart card authentication:

1. On the Red Hat Linux computer, run the following command to check the status of smart card support:

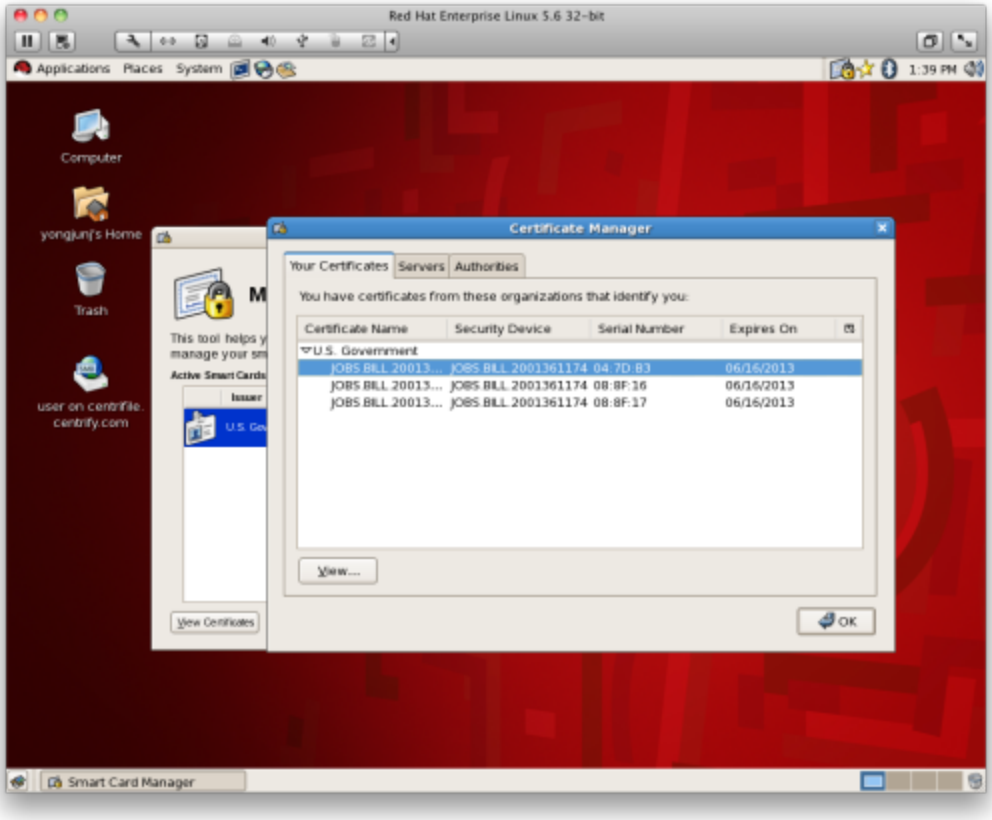
   `[root]#sctool --status` DirectControl Smart Card support is enabled.

   > On Red Hat Linux computers, when enabling smart card support, the agent bypasses the native, Red Hat, smart card infrastructure. Therefore, after you enable smart card with the agent (through the group policy setting or the `sctool` command), the `sctool --status` command will show that smart card is enabled but the Red Hat system (GNOME: System > Administration > Authentication > Authentication) might show that it is not enabled. You can ignore the GNOME setting because it is for native smart card authentication, not the authentication used by the agent.

2. Click **System > Administration > Smart Card Manager**.



3. Insert the smart card in the reader and click **View Certificates**.
4. Double-click the certificate for a user account that has a profile in the zone the Red Hat Linux computer has joined, for example, **JOBS.BILL.20013**.



5. Scroll to find the NT Principal name; for example:

   NT Principal Name jbill.20013@myDomain.com

6. On a Windows computer, open Activity Directory Users and Computers or the Access Manager console. For example, in the Access Manager console, navigate to the zone that the Red Hat Linux computer has joined and open **UNIX Data > Users**, then double-click the user.

   The NT Principal name in the certificate should match the login name in the Delinea UNIX profile, or in the Active Directory Account tab.

7. Log out of the Red Hat computer.
8. Re-insert the smart card in the reader and enter the user's PIN.

Using a Smart Card at Login

When a user inserts a smart card into the card reader attached to a Red Hat Linux computer that is waiting for login, the login dialog is replaced by a smart-card enabled login (if the card is provisioned for an Active Directory user who is enabled for the Delinea zone to which the computer is joined). However, the actual log on screen varies depending on whether the card is provisioned for a single user or for multiple users.

How the Login Screen Appears for a Single-User Card

When a user inserts a single-user card, the smart card login shows the name of the user for whom the card is provisioned, and provides a single text box in which the user can type the PIN associated with the card.

If the user is not enabled for the zone, or is not a valid Active Directory user at all, the smart card login screen is replaced by either a list of local users, or user name and password text entry fields.

The user will be successfully logged in if the following conditions are met:

- The user enters the correct PIN for the smart card.
- The card is trusted by the domain and has not been revoked. The card is checked locally first, online or offline, to ensure that the issuing certificate authority is trusted by the Red Hat Linux computer through the certification authority trust chain, which is set up when the computer joins the domain, and is periodically refreshed.

Checking is performed by the domain controller when the computer is online, and by a local service, based on cached CRLs, when the computer is offline. If the user is not connected to the network but has previously logged on – with a smart card or in some other way – the Delinea Agent gets the UPN from the card and looks up the user in the cached data.

If login fails, no feedback is provided to the user as to why the login is being denied. However, information is logged into various system log files, /var/log/system.log, /var/log/secure.log, and the Delinea log file (/var/log/centrifydc.log) if logging is enabled, that can help determine the reason for a denied login.

How Login Screen Appears for a Multi-User Card

When a user inserts a card that is provisioned for multiple users, the smart card login provides a **Username** box that allows the user to enter the name of the account to use.

When the system finds the user account in Active Directory, it prompts the user to enter the PIN for the card.

If the user is not enabled for the zone, or is not a valid Active Directory user at all, the smart card login dialog is replaced by the previous login screen, either a list of local users or username and password text entry fields.

The user will be successfully logged in if the following conditions are met:

- The user enters the correct PIN for the smart card.
- The card is trusted by the domain and has not been revoked. The card is checked locally first, online or offline, to ensure that the issuing certificate authority is trusted by the Red Hat Linux computer through the certification authority trust chain, which is set up when the computer joins the domain, and is periodically refreshed.

Checking is performed by the domain controller when the computer is online, and by a local service, based on cached CRLs, when the computer is offline. If the user is not connected to the network but has previously logged on – with a smart card or in some other way – the Delinea Agent gets the name from the log on screen and looks up the user in the cached data.

If login fails, no feedback is provided to the user as to why the login is being denied – as is the case when logging in with a password. Information is logged into various system log files that can help determine the reason for a denied login, /var/log/system.log, /var/log/secure.log, and the Delinea log file (/var/log/centrifydc.log) if logging is enabled.

Screen Saver Shows Password Not PIN Prompt

Most smart card users are allowed to log on with a smart card and PIN only – they cannot authenticate with a user name and password. However, it is possible to configure users for both smart card/PIN and user name/password authentication. Generally, this set up works seamlessly: the user either enters a user name and password at the log on prompt, or inserts a smart card and enters a PIN at the prompt.

However, for multi-user cards, it can be problematic when the screen locks and the card is in the reader. When a user attempts to unlock the screen, the system prompts for a password, not for a PIN, although the PIN is required because the card is in the reader. If the user is not aware that the card is still in the reader and enters his password multiple times, the card will lock once the limit for incorrect entries is reached.

What Happens After Login

In general the user experience is the same in both connected and disconnected modes, with the exception of single sign-on (SSO). Because the agent does not cache the smart card's PIN, single sign-on (SSO) is available for smart card authentication only while the computer is connected to the domain.

Of course, certain behaviors and system responses are specific to smart card login:

- If the user removes the smart card after logging on, the response of the system depends on whether the group policy "Lock smart card" screen is enabled in the domain. If it is, the screen locks. Otherwise, the screen does not lock and the user may continue working.

  > For a smart card that is provisioned for multiple users, if the screen locks, the system prompts for a Password, not for a PIN, when the user logs back in. However, the user must enter the PIN for the card, *not* the password, when logging back in.

- If the user inserts a smart card while the screen saver is active, the response depends on whether "Lock smart card screen" is enabled in the domain. If it is, the screen saver deactivates. If the policy is not enabled, the screen saver continues running until the user moves the mouse or touches a key.

Disabling Smart Card Support

If you want to disable smart card support, you must disable the group policies you configured to establish smart card authentication.

To Disable Smart Card Support by Using Group Policy

1. Edit the Group Policy object linked to the site, domain, or OU that includes Red Hat Linux computers.
2. Expand **Computer Configuration** > **Policies** > **Centrify Settings** > **Linux Settings**, click **Security**, then double-click **Enable smart card support**.
3. Select **Disabled** and click **OK**.

   When the policy takes effect, smart card strings are removed from `/etc/pam.d/system-auth` on Red Hat Enterprise Linux 5.6 and `/etc/pam.d/smartcard-auth` and `/etc/pam.d/gnome-screensaver` on Red Hat Enterprise Linux 6.0.
4. Expand **Computer Configuration** > **Policies** > **Centrify Settings** > **Linux Settings**, click **Security**, then double-click **Lock Smart Card screen for RHEL**.
5. Select **Disabled** and click **OK**.
6. To apply these group policies immediately to any computer, restart the computer or run the `adgpupdate` command on it.

   Otherwise, all affected computers will be updated automatically at the next group policy update interval. After computers are restarted or receive the policy updates, they are no longer enabled for smart card use.

To Disable Smart Card Support by Running sctool

1. Log on to a Red Hat computer with root privilege and open a terminal window.
2. Run the `sctool` utility with the `--disable` option:

   ```
   [root]$ sctool --disable
   ```
3. Repeat steps 1 and 2 for each computer on which to disable smart card authentication.

> If you originally enabled smart card support through group policy by setting “Enable smart card support” you cannot disable it by using `sctool --disable`. Although this command will temporarily disable smart card support, it will be re-enabled by the policy at the next group policy update interval. To permanently disable smart card support, you must disable **Enable smart card support** as described in the previous procedure, To disable smart card support by using group policy.

Troubleshooting Smart Card Login

If you have problems with smart card login, Server Suiteprovides a command-line tool, `sctool`, that you can run to configure smart card login, as well as to provide diagnostic information. For example, you can run `sctool` with the following options:

- `sctool --status` to show whether smart card support is enabled.
- `sctool --dump` to display information about the smart card system setup as well as any smart cards that are attached to the computer.
- `sctool --pkinit`*userPrincipalName* to obtain Kerberos credentials on a single-user smart card for troubleshooting purposes.

  During login with a smart card, the agent calls `sctool --pkinit` to obtain Kerberos credentials from the smart card currently in the reader. Because this option simulates a good portion of the smart card login process, if you are having trouble logging in you can run `sctool --pkinit` to obtain useful troubleshooting information. If the command executes successfully, the name of the user will be displayed. If the command fails, you will receive an error message that may help you troubleshoot the issue.
- `sctool --altpkinit`*unixName* to obtain Kerberos credentials on a multi-user smart card for troubleshooting purposes.

  During login with a multi-user smart card, the agent calls `sctool --altpkinit` to obtain Kerberos credentials from the smart card currently in the reader (because the card is configured for multiple accounts, the user is prompted to provide a username, which the command uses to obtain the Kerberos credentials). Because this option simulates a good portion of the smart card login process, if you are having trouble logging in you can run `sctool --altpkinit` unixName to obtain useful troubleshooting information. If the command executes successfully, the name of the user will be displayed. If the command fails, you will receive an error message that may help you troubleshoot the issue.
- `sctool --check-kdc-eku` to enable checking of the KDC certificate for the Extended Key Usage (EKU) extension "Kerberos Authentication". Do not use this option if you have not updated your KDC to include the required EKU. Enable EKU checking after updating your KDC certificate.

EKU checking is disabled by default.

This parameter must be used with the `-k (--pkinit)` parameter or the `-a (--altpkinit)` parameter

For more information about using sctool, see the sctool man page.