

6.2. Enabling Smart Card Login on Red Hat Enterprise Linux

Smart card login for Red Hat Enterprise Linux servers and workstations is not enabled by default and must be enabled in the system settings.

NOTE

Using single sign-on when logging into Red Hat Enterprise Linux requires these packages:

- nss-tools
- esc
- pam_pkcs11
- coolkey
- ccid
- gdm
- authconfig
- authconfig-gtk

1. Log into the system as root.
2. Download the root CA certificates for the network in base 64 format, and install them on the server. The certificates are installed in the appropriate system database using the `certutil` command. For example:

```
certutil -A -d /etc/pki/nssdb -n "root CA cert" -t "CT,C,C" -i /tmp/ca_cert.crt
```

3. In the top menu, select the **System** menu, select **Administration**, and then click **Authentication**.
4. Open the **Authentication** tab.
5. Click the **Enable Smart Card Support** checkbox.
6. When the button is active, click **Configure smart card**

There are two behaviors that can be configured for smart cards:

- The **Require smart card for login** checkbox requires smart cards and essentially disables Kerberos password authentication for logging into the system. This should not be selected until *after* you have successfully logged in using a smart card.
 - The **Card removal action** menu sets the response that the system should take if the smart card is removed during an active session. Ignore means that the system continues functioning as normal if the smart card is removed, while Lock immediately locks the screen.
7. By default, the mechanisms to check whether a certificate has been revoked (Online Certificate Status Protocol, or OCSP, responses) are disabled. To validate whether a certificate has been revoked before its expiration period, enable OCSP checking by adding the `ocsp_on` option to the `cert_policy` directive.

- Open the `pam_pkcs11.conf` file.

```
vim /etc/pam_pkcs11/pam_pkcs11.conf
```

- Change every `cert_policy` line so that it contains the `ocsp_on` option.

```
cert_policy =ca, ocsp_on, signature;
```

NOTE

Because of the way the file is parsed, there *must* be a space between `cert_policy` and the

equals sign. Otherwise, parsing the parameter fails.

8. If the smart card has not yet been enrolled (set up with personal certificates and keys), enroll the smart card, as described in [Section 5.3, “Enrolling a Smart Card Automatically”](#).
9. If the smart card is a CAC card, the PAM modules used for smart card login must be configured to recognize the specific CAC card.
 - As root, create a file called `/etc/pam_pkcs11/cn_map`.
 - Add the following entry to the `cn_map` file:

```
MY.CAC_CN.123454 -> login
```

MY.CAC_CN.123454 is the common name on the CAC card and *login* is the Red Hat Enterprise Linux login ID.

TIP

When a smart card is inserted, the `pklogin_finder` tool (in debug mode) first maps the login ID to the certificates on the card and then attempts to output information about the validity of certificates.

```
pklogin_finder debug
```

This is useful for diagnosing any problems with using the smart card to log into the system.