```
=====================================================
iSD-SSL 4.2.1.11
Released on 18 october 2004
=====================================================

Enhancements
------------
The port forwarder and proxy Applets now support automatic proxy
  configuration scripts. This when running Internet Explorer (IE).

  Background:
  IE can be configured to use automatic proxy scripts. Configured from here:
  "Tools -> Internet Options -> Connections -> LAN Settings ->
   Use automatics configuration script"

  If so IE downloads and evaluates the configuration script (PAC file)
  to figure out which proxy to use.

  If you want more info on PAC files read more here:
  http://wp.netscape.com/eng/mozilla/2.0/relnotes/demo/proxy-live.html

  How it works:
  If IE has been configured to use a PAC file the Applets do the same as
  the browser, i.e. it downloads the PAC file and evaluates it to
  figure out which proxy to use. Nothing has to be enabled in our CLI/BBI.

Fixes
-----
Added code to handle iauto forms which are broken, ie missing </form>.

Fixed problem with javascripts that performed document.open
  Some of our variables were lost resulting in links on the form
  undefined://undefined/http/....

Fixed problem with securecookie in SSL acceleration mode.
  The Secure option was not added to Set-Cookie headers generated
  by the backend server when the /cfg/ssl/server #/http/securecookie
  option was on for type=http servers.

Fixed problem with ,xct1 and ,xct2 in javascript urls.

Fixed problem with document.writeln
  We did not handle writeln properly in some unusual circumstances
  when the newline was relied on to create spaces between tag options,
  ie,
        doucment.writeln("<img src='foo'");
        document.writeln("alt='some image>');

New version of the IE-wiper, 1.0.0.21.
  Error in the registrymapping solved, related to "IEWiper removes the typed
  URLs" problem.

Disk repartitioning support for upgrade to version 5.0.
  On some ASA systems, the disk will need to be repartitioned to make it
  possible to upgrade from 4.2.x to 5.0 - support for this has now been
  added. The Release Notes for version 5.0 will provide further details.

=====================================================
iSD-SSL 4.2.1.10
Released on Oct 7 2004
=====================================================

Enhancements
```

Added command to turn off ClearAuthenticationCache for IE
/cfg/ssl/server #/portal/ieclear <on/off>

Added command to allow caching of scripts
/cfg/ssl/server #/http/allowscript <on/off>

Automatically add host in ssodomain when an ftp and smb link is created.

Added /cfg/ssl/server #/portal/ieclear to control clearing of the authentication cache in IE

Backported dynheader from 5.0
This makes it possible to add custom headers to the requests passing through the ASA. The new commands are

```
/cfg/ssl/server #/http/dynheader
/cfg/ssl/server #/http/dynheader/add
/cfg/ssl/server #/http/dynheader/del
/cfg/ssl/server #/http/dynheader/list
/cfg/ssl/server #/http/dynheader/insert
/cfg/ssl/server #/http/dynheader/move
```

You specify for which domain (or fqdn) a header should be added. The header may contain macros which are expanded when the header is added. For example

```
/cfg/ssl/server 2/http/dynheader/.
        add * "X-cert: client cert <var:clicert>"
```

will add the header X-cert to all backend servers. <var:clicert> will be expanded to a base 64 encoded version of the clients certificate, if one is present.

The following macros are available:

<var:method>	http or https
<var:sslid>	SSL session id in binary format
<var:clicert>	Base 64 encoded client certificate
<md5:...>	Will expand ... and then compute an md5 checksum which is base64 encoded
<base64:...>	Will expand ... and then encode it using base64

Fixes

Fixed problem with compressed content.
We previoiusly removed the Accept-Encoding: gzip, deflate header even when we can handle it. We now keep the header to allow the backend server to send compressed content.

The http proxy Applet wizard in the CLI now uses iexplore.exe to open a new browser after the Applet has started. Previously it used a Java internal library call, i.e. the auto reconfiguration of the browser proxy wan't recognized by the new window in that case.

Fixed Q00956086: Lingering listen socket now removed for the Outlook and HTTP proxy Applets

Fixed problem which caused all users to be logged out
If the ASA queried the user for username and password for Basic backend authentication, and the user checked the 'save password as default' checkbox, then all users would be logged out from the ASA.

Fixed 00952235-01: iauto login to pages that contained multiple forms

Made sure the ASA doesn't touch Pragma and Cache-Control
  Pragma and Cache-Control headers are only modified
  for VPN (portal) servers and for http servers when the
  allowdoc setting is turned on.

Fixed problem with http to https redirect
  The ASA genereated redirects containing explicit port
  numbers when that wasn't needed, which confused some
  browsers. Now port information is only included when
  needed.

Fixed problem with importing oneline base64 encoded certificates

Fixed problem with duplicate cookies

==========
iSD-SSL 4.2.1.9
Released on Sept 17 2004
==========

Fixes

Fixed problem with Microsoft SharePoint SOAP interface

Fixed traffic subsystem restart issue
  The traffic subsystem could restart when a backend server made
  heavy use of NTLM authentication.

Fixed javascript rewrite error
  The ASA would fail to rewrite javascript and HTML properly
  if a quoted element occured as first entry in a regular expression,
  eg,
        str = str.replace(/\'/g, "\'\'");

Fixed potential loss of default gateway setting
  Some network reconfigurations (e.g. changing port number for the
  interface used to reach the default gateway) could effectively
  disable the default gateway setting.

Fixed Q00956755; Cannot import CleanupNortelRPC.reg error upon bootup.

==========
iSD-SSL 4.2.1.8
Released on Sept 16 2004
==========

Fixes

Fixed minor dynamic html rewrite bug related to domain
  cookies set from javascript.

Fixed Q00920659 and Q00921624; connection aborts when
  running activex or java citrix clients.

Fixed problem with Citrix form based login.

Fixed minor bug in http to https redirect. It is not
  possible to write $(host):<port> as to host.

Fixed problem with iauto login to Citrix. Added cookie
option to iauto wizard and a cookies submenu in
/cfg/xnet/domain #/group #/link #/iautoconf.

Better LDAP trace printout when no matching user found.

Fixed type checking of LDAP IP address and valid Port range.

Fixed Q00905635; apply of incomplete configuration (no certificate specified) generated an internal message.

Fixed intermidiate squid authentication prompt, Q00956089.

Added support for pre-set cookies for iauto form link
Some servers requires the client to have certain cookies present to send a login form to the user, eg Citrix. We have added support for this. It is now possible to optionally specify a list of cookies to send to the backend server when retrieving the login form. A new submenu has also been added to edit these values.

/cfg/xnet/domain #/group #/link #/iautoconf/cookies

Fixed generation of testcertificates from BBI, Q00972300.

Fixed Q00930299-01; importing PEM certificates with key and/or cert on one row.

Fixed Q00959481-01; Handle Set-Cookie headers in sso basic authentication.

Fixed Q00959019-1; ssodomains now works with shortnames and ip addresses in the request.

Fixed Q00952600; if a NTLM pasword-expired group is triggered, then no other groups will used.

Fixed Q00935383; multiple group attribute names.

The macros in the static linktext are no longer url encoded.

Fixed Q00887962; ssldump caused internal error message to display on console.

Fixed Q00949685; Box in standalone configuration - access to BBI even if client is not part of ACL.

Fixed Q00949685; Don't allow "direct" management access via standalone server IP.

BBI updates;
The primary change is we now hide the passwords that are typed for RADIUS and Local User authentication (i.e. a password field is used and the text is asterixed out).

Socks tcp sessions are no longer aged using tcpKeepAlive
We no longer age socks tcp sessions, we instead rely on the aging of portal sessions.

Added workaround for broken backend server.
If a backend server fails to send a status code in the response we now assume that it is 200 OK.

Fixed problem with XML/XSL rewrite.
  Added a fix for rewriting them XML stylesheet href.

Fixed problem with " in javascript tag values
  We did not properly handle quoting using " in
  javascript tags, for example

      <body onLoad='test1="hej";test2["hop"]=bar;'>

  is a valid javascript which we now handle.

Fixed rewrite problem with dynamically generated HTML
  Dynamically generated HTML was not correctly rewritten
  if a tag had a non-value attribute in front of an attribute
  that should be rewritten. Eg

        document.write("<a nospace href='/filur/bar.html'>")

  would not be properly rewritten due to the nospace attribute.
  This is now fixed.

Don't allow direct management access via standalone SSL server IP address
  When using SSL server "standalone" IP addresses that didn't fall
  within any configured interface subnet, it was possible to get direct
  access to management CLI/BBI through these addresses, regardless of
  access list configuration. This has now been blocked, and these
  addresses never give direct management access. (Q00949685)

Allow direct management access via additional "private" interfaces
  Previously, direct access to management CLI/BBI was only possible
  through the management interface (interface 1), and only using the MIP
  address, or the IP address assigned to the management interface. This
  restriction has been partially lifted, and such access is now possible
  via all interfaces except for the "traffic" (i.e. "public") interface
  (when different from the management interface).

Support new flash disk partitioning scheme on AAS 2424-SSL
  The upcoming SSL-5.0 release will require repartitioning of the flash
  disk on AAS 2424-SSL for full functionality (further information will
  be in the 5.0 Release Notes). The new partitioning scheme is supported
  as of this release.

==========
iSD-SSL 4.2.1.7
Released on 10 Aug 2004
==========

Enhancements

Added DNS name resolution failure to /maint/starttrace.

Added ssodomains to limit to which backends the ASA tries to
  automatically login. Previously the ASA would try to login
  to an ftp server using the users default passwords, without
  first prompting the user. This could be used to obtain password
  without the user knowing. SSODomains are also used to
  specify to which backends the ASA should automatically login
  without first specifying an iauto link.

Made it possible to have a path in dhost
  It is now possible to have a path part in the dhost setting

  for portals with authentication turned off.

Fixes

Updated wiper to 1.0.0.20

Fix to the Outlook port forwarder Applet: Now restores the
  Rpc_Binding_Order correctly.

Fixed bug in matching of ssodomains

Fixed problem with quotation marks in html comments in javascripts.

Fixed problem with Set-Cookie in WWW-Authenticate response from the
  backend. These cookies are now collected and sent to the backend in
  the authentication handshake, and then sent to the client at the end
  of the authentication handshake.

Fixed problem with rewriting links with many trailing spaces
  Links that were rewritten into links ending with ,xct2 were
  rewritten to include trailing whitespaces. These whitespaces
  are now removed.

Fixed problem with domain cookies generated from javascript

Fixed Case 040511-49031
  Hrefs with initial newlines were not rewritten properly.

Fixed security problem with session cookie
  The ASA will now by default set the secure option
  on the session cookie and all set-cookie headers
  generated by backend servers. This behaviour can
  be controlled by /cfg/ssl/server #/http/securecookie <on/off>
  The old behaviour is 'off'.

Fixed CR Q00942128: SSL Server standalone can only service 1 ip

Fixed Cross-Site Scripting vulnerability.

Fixed problem with binary data in X-SSL header
  The ssl_sid value is now hex encoded

Fixed problem with formating of X-SSL subject and issuer
  We now follow RFC 2253 when formating subject and issuer in
  the X-SSL header. This is a potential incomparability with
  previous releases.

Fixed rewrite problem of base tags in html on the form
  'http://host'.

The Outlook port forwarder Applet has been changed in accordance with
  http://support.microsoft.com/default.aspx?kbid=325930, i.e. the
  Rpc_Binding_Order registry value is now set to "ncacn_http"
  only. Previously other communinication mechanisms were preserved
  as well, e.g. "ncacn_http,ncacn_ip_tcp,ncacn_spx,ncacn_np,netbios".
  This change avoid nasty failover to rpc mechanisms not being available
  in a VPN scenario.

  The details:

  * If SavedOrder (see below) is set the Outlook reconfiguration has

already been done, i.e. the Applet does nothing with the Order and SavedOrder keys.

* If SavedOrder is *not* set. The Applet:

1) Copies Order into SavedOrder and sets Order = "ncacn_http".
2) Creates a regedit file named %TEMP%\CleanupNortelRPC.reg. This regedit file replaces Order with SavedOrder and deletes the SavedOrder key (when being evaluated).

* On termination the Applet copies SavedOrder (if any) to Order and sets SavedOrder to "". The regedit file is removed as well.

* On client reboot the CleanupNortelVPN.bat script, in the Startup folder, has been extended to evaluate the regedit file and after that remove it.

Order = HKLM\SOFTWARE\Microsoft\Exchange\Exchange Provider\Rpc_Binding_Order
SavedOrder = HKLM\SOFTWARE\Microsoft\Exchange\Exchange Provider\Saved_Rpc_Binding_Order

==========
iSD-SSL 4.2.1.6
Released on 28 June 2004 (public)
==========

Extention to the documentation

** New Citrix Support **
/cfg/xnet/domain #/portal/citrix on|off
Enables/disables support for Citrix Metaframe links on the Portal.

on: Makes it possible to configure a Portal link to a Citrix Metaframe server by simply specifying the URL with the "internal" link command. This link type directs the request to the SSL where the SSL rewrite prefix is added to the link.

off: Links to Citrix Metaframe servers can only be created by means of the "citrix" port forwarder link type. If Citrix Metaframe links are not used, "off" is the recommended setting, since this saves the SSL from starting the applet that supports this feature.

Note: When "citrix" is set to "on", the SSL supports rewrite of ICA files only. Other methods are possible but may require configuration changes on the Citrix Metaframe server side.

The default value is off.

** RSA native authentication **
RSA authentication is configured as described below.

1. Specify an RSA server in the '/cfg/sys/rsa' menu by setting a symbolic server name and importing an 'sdconf.rec' file from the RSA server.

2. Configure the ASA to use RSA authentication in the '/cfg/xnet/domain #/auth #/rsa' menu by setting 'rsaname' to the server name specified above and setting 'rsagroup' to a user group defined on the ASA. All RSA authenticated users will be assigned to this group.

  If needed, the RSA node secret can be removed with
  '/cfg/sys/rsa #/rmnodesecr'. Authentication will then fail until the
  check box 'Node secret created' is unchecked in the 'Edit Agent Host'
  at the RSA server.

Fixes

When /cfg/xnet/domain #/portal/citrix was changed, it had
  no effect until a restart. This is now fixed.

The citrix applet no longer tries to resolve hostnames on the
  client machine.

Fixed Q00919607-01 - escape \ in username and passwd to the
  full access applet.

==
iSD-SSL 4.2.1.5
Released on 22 June 2004 (for QA)
==

Fixes

Timeout set to 5 minutes for a rsa challenge interaction.

Improved control of rsa processes.

==
iSD-SSL 4.2.1.4
Released on 21 June 2004 (for QA)
==

Enhancements

Added rewriting of ftp links
  An ftp link that occur on a webpage will be rewritten
  as https://portal.com/xnet/ftp/<host><path>

Fixes

Native RSA support partly rewritten. Part 1 of the CR Q00930910 is fixed.

Updated webUI
  1. 'Native RSA' in 'Administration->RSA Servers' page
  2. '/cfg/ssl/server #/sslxheader' in 'SSL->Servers->Types->HTTP->General' page
  3. 'character set in use' in 'SSL-VPN->Domains->Portal->Language' page
  4. '/cfg/ssl/server #/http/httpsredir' in 'SSL->Servers->Types->HTTP->HTTPS
Redirect' page
  5. '/cfg/ssl/server #/http/redirmap' in 'SSL->Servers->Types->HTTP->HTTPS
Redirect' page
  6. 'Confirm Logout' and 'Citrix Support' in 'SSL-VPN->Domains->Portal->General'
page
  7. Fix for strange appearance bug reported by Katrin on 14th June

Fixed bad error message: Unknown POSIX error.

Fixed CR Q00911381-01

Improved Citrix support, removed reverse lookup in Citrix SOCKS applet,

  content length used for ica files, on/off in CLI.

Fixed FIN retransmit to clients using wrong source address
  In some (rare) cases when the client didn't ACK the final data
  and FIN sent from the ASA on session close, the ASA could, after
  multiple retransmits without ACK, do subsequent retransmits using
  the ASA's own IP address as source address instead of the VIP.

==========
iSD-SSL 4.2.1.3
Released on 3 June 2004 (for QA)
==========

Fixes

Fixed iauto proxy validation.

==========
iSD-SSL 4.2.1.2
Released on 2 June 2004 (for QA)
==========

Enhancements

The logout behaviour has been made configurable
  It is now possible to configure weather logout should
  be confirmed or not. It is done using the cli command
  /cfg/xnet/domain #/portal/confirm <true|false>

Fixes
=====

Fixed problem with UDP port forwarder
  The applet was broken and would not properly forward
  packets from the remote side. They were truncated
  and sometimes an error showed up in the java console.

Fixed problem with SSL_connect to 127.0.0.1:8000

Fixed problem with unwanted rewrites of pdf files

Fixed problem with https rewrite for type http servers
  If the http server used odd ports then the backend
  redirect would not be rewritten. For example, if the
  https server used port 8100 and the backend server used
  port 82, then a redirect from the bakend server to
  http://vip:8100 would not be rewritten.

  Also, if http/rhost and http/defaulthost was set with
  port information, then the listen port would still be
  added to the host header. This made it impossible to
  rewrite a host header with port information. This has
  also been fixed.

lib/ssl_cli:
    Fixed Q00916934 - make citrix portal command non-hidden. Made
  citrix pfwd link command hidden instead.

lib/aaa:
  Fixed Q00914982 chkcfg on old link formats could crash the cli.

lib/oam_snmp:
  Fixed snmp problem for get with bad oids (oids for objects which are
  guaranteed to not exist).

lib/portal:
  Removed passwords from Java console for the full access Applet.

lib/portal:
  Fixed logout problem when going through proxy Applet

lib/oam_snmp:
  Bugfix of get_next. Robustification against unexpected inputs.

lib/portal:
  Fixed Q00911774

lib/simpleproxy:
  Fixed Q00909202: iauto in proxy mode didn't work the first time.

lib/ssl_cli:
  Fixed Q00908918 -   'cur' under an NTLM auth server gives Internal
  error.

lib/simpleproxy:
  Fixed problem with   redirect for type http servers. If the server was
  run on an odd   port then the redirect message from the backend server
  would not   be proberly rewritten.

lib/portal:
  Fixed lycos mail login.

lib/portal:
  Fixed problem with hosts/lmhosts files updating.

==========
iSD-SSL 4.2.1.1
Released on May 14 2004 (for QA)
==========

Enhancements

Added support for creating 4096 bit certificates

Added http to https redirect settings
  You can create an http to https redirect server (in a much
  easier way than before). This is done by configuring an http server,
  turning off ssl and enabling https redirect

         /cfg/ssl/server #/http/httpsredir on

  This will case all requests to that server to be redirected
  to https with the same host and path as the original request.

  It is also possible to configure host->host mappings, so that
  a request for http://host1[:Port1]/Path will be redirected to
  https://host2[:Port2]/Path

  This is done using the /cfg/ssl/server #/http/redirmap setting.

  This setting can also be used to create more advanded redirect

patterns using two builtin varialbes $(host) and $(path), and
the matching pattern '*'. Using '*' as host1 in the mapping
will match all hosts.

For example, if you want to create a redirect pattern that causes all
requests to be directed through a portal you would use the following
pattern (provided that your portal is test183.bluetail.com.

```
>> Redir Map# list
     1: test183.bluetail.com "https://test183.bluetail.com/$(path)"
     2: * "https://test183.bluetail.com/http/$(host)/$(path)"

>> Redir Map#
```

The effect of this pattern is that requests to test183 will be https
redirected to test183, and all other requests will be redirected
to the original host but through the portal.

This feature is useful if you configure your external DNS to point
all internal names to this redirect server. You can then
use all your browser bookmarks both internally and externally
though the portal, you can also click directly on links that you
receive through, for example, an email.

Added support for controling behaviour when server is down
Added new cli command to control the reply message when server is down
It is now possible to control the reply message sent to the
client when a backend server is down using the command

```
/cfg/ssl/server #/http/downstatus
```

Possible values are 'unavailable' (default), 'redirect', and
'reset'. When 'redirect' is selected you can configure a redirect
url using the setting

```
/cfg/ssl/server #/http/downurl
```

Added portal support for Citrix NFuse, which should be used instead of
starting special citrix port forwarders. To enable citrix support on
the portal, type /cfg/xnet/domain #/portal/citrix on. When a user
logs in, a citrix applet will be started. When the user clicks on a
ica file, the file is rewritten on-the-fly so all connections are
tunneled through the new applet. The ica files must not be modified
for the portal, they should contain the normal ip addresses etc.

Note that old citrix port-forwarder links must be removed, they will
not work. To recreate such a link, create an 'internal' link which
points to the nfuse page.

Merged Native RSA support from SSL-4-1-2-11

It is now possible to check the query part in acl paths for http
requests. The syntax for such a path is "/foo*?cmd=*". This means
that you can specify a prefix for the path part of the url, and a
prefix for the query part.

Fixes

Added cookie wiping code for IE 6 SP1 and later
Cookies are always removed when the browser is closed but
with this fix they will be removed as soon as you exit the

portal even if the portal isn't closed. This prevents
problems if another user logs in from the same browser
to the same portal without closing the browser in between.

A bug was corrected where it was not possible to run several
(more than one) ssl servers with _different_ portnumbers, same VIP list
and at the same time using standalone mode.

Fixed CR-Q00890008:
SSL-VPN: max number of domains is now changed to 256

Fixed CR-Q00886949 and CR-Q00886820; now the cur, curb, dump, diff,
apply, /cfg/gtcfg and /cfg/ptcfg commands does not have a CLI timeout

The BBI now contains the Netdrive bug fix.

Fixed CR-Q00882370: Took too long to login to CLI if unreachable
DNS servers were configured (we tried to reverse lookup the name
of all logged in admin sessions.

Fixed CR-Q00891858: /maint/chkcfg now handles all link formats.

The defualt group specified in /cfg/ssl/server #/portal/dgroup may now
contain spaces.

Fixed CR-00886176: If an NTLM auto login results in a 302, it was not
automatically followed, so the user ended up on the new page where
they had to manually login.

Rewrite fix: now handle the web interface to windows terminal
services.

Rewrite fix: do not rewrite explict links to files on the portal,
e.g. logout.yaws.

Fixed CR-Q00883621.

Fixed CR-Q00834510.

Fixed CR-Q00881738.

Fixed problem with IE proxy settings
Fixed problem with IE proxy settings set via
"Tools -> Internet Options -> Connections -> LAN Settings"
when using the SSL VPN port forwarder applet. Now both configuring IE
proxy via
"Tools -> Internet Options -> Connections -> LAN Settings" and
"Tools -> Internet Options -> Connections -> LAN Settings -> Advanced..."
works.

Fixed problem that caused the user to be logged out of the portal
when logging out from OWA 2003.

Fixed problem which caused pure VB-Script pages to not be rewritten

Fixed problem with automatic configuration of iauto forms
Some server deliver different pages depending on the
User-Agent header which caused problems when running the
iauto wizard since the ASA didn't send any User-Agent at all.
The ASA now masquerades as IE 6.0. Also, support for
radio buttons in the login form has been added.

Fixed bug with using iauto and a proxy server

Fixed problem with security warning when logging out of portal

Fixed problem with login when accessing intranet links
  A bug was introduced in 4.2 which caused direct access to
  intranet sites to be broken. The expected behaviour when
  accessing a link like

        https://portal.foo.com/http/intranet.foo.com/index.html

  without first having logged in is to get the login page.
  This did not work in 4.2 and has now been fixed.

Fixed problem with images as topmost elements of a frame
  The topmost content of a frame was assumed to be html
  and would sometimes be falsely rewritten. This has now
  been fixed.

Fixed problem with client certificates for non-portal servers
  Non-portal servers could not be configured to require
  client certificates.

==========
iSD-SSL 4.2.1
Released on May 10, 2004
==========

For release information of the SSL-4.2.1 release, please refer to the "Release Notes" document accompanying the SSL-4.2.1 release. This README describes changes in the following releases.

==========
Software Installation and Upgrade Notice
==========

The software is delivered in two different forms, as described below.

- SSL-4.2.x-upgrade_complete.pkg

  Using this package is the preferred method for upgrading an existing SSL VPN cluster, as the upgrade is propagated across the cluster and all current configuration is preserved.

  The upgrade procedure is described in "Performing Minor/Major Release Upgrades" in Chapter 4 in the SSL VPN User's Guide.

- SSL-4.2.x-boot.img

  Using this image will reset the SSL VPN device to its factory default configuration. It must be used when an SSL VPN device with different software installed is to be added to a cluster, to bring the additional SSL VPN device to the same software version as in the cluster before joining it to the cluster.

  The software reinstall procedure is described in "Reinstalling the Software" in Chapter 3 in the SSL VPN User's Guide.

Compatibility Issues

The SSL VPN authentication method 'rsa' that was introduced in software version 4.1.2.7 is NOT supported in version 4.2.1. Upgrading to 4.2.1 of an SSL VPN cluster configured for RSA authentication will fail.
RSA support was reintroduced in version 4.2.1.1 so upgrade/downgrade when 'rsa' is configured will work between 4.1.2.7 and 4.2.1.1 and later versions, but not with version 4.2.1.

The SSL VPN authentication methods 'cert' and 'siteminder' were introduced in software version 4.2.1. Downgrading to a lower version number of an SSL VPN cluster with any of these authentication methods configured will fail.

Upgrading from Versions Earlier than 2.0.11.15

If you are currently running a software version earlier than 2.0.11.15, upgrade to version 2.0.11.15 (or a later 2.0.11.x version) prior to upgrading to version 3.x or later. The "intermediate" upgrade to version 2.0.11.15 is necessary in order to maintain your current configuration, and to provide reliable fallback in case the upgrade should fail.

Downgrading to Versions Prior to 4.1.1

SSL VPN clusters running software version 4.1.1 or later cannot be downgraded to software versions prior to 4.1.1 and still retain the configuration. To downgrade such a cluster to a version lower than 4.1.1, a complete software reinstall using the boot.img must be performed, followed by manual reconfiguration of the cluster. This is due to changes in the internal database format.

Reverting to 4.2.1 or Higher after Downgrading to 4.1.x

An SSL VPN cluster running software version 4.2.x can be downgraded to version 4.1.1 or higher. However, after downgrading a cluster initiated with software version 4.2.1 or higher to version 4.1.x, the cluster cannot be upgraded to version 4.2.1 or higher and still retain the configuration. To revert the downgraded cluster to version 4.2.1 or higher, a complete software reinstall using the boot.img must be performed, followed by manual reconfiguration of the cluster. This is due to changes in the internal database format.