



VIEWDS VERSION 7.4 PATCH 5  
RELEASE NOTES

ViewDS Version 7.4 Patch 5 Release Notes

August 2017

#### **Document Lifetime and User Experience**

ViewDS may occasionally update online documentation between software releases. Consequently, this PDF may not contain the most up-to-date information. In addition, links to other ViewDS documents contained in this PDF will not work. Refer to the online documentation at [www.viewds.com/resources/documentation.html](http://www.viewds.com/resources/documentation.html) for the most current information and a better browsing experience.

This publication is copyright. Other than for the purposes of and subject to the conditions prescribed under the Copyright Act, no part of it may in any form or by any means (electronic, mechanical, microcopying, photocopying, recording or otherwise) be reproduced, stored in a retrieval system or transmitted without prior written permission. Inquiries should be addressed to the publishers.

The contents of this publication are subject to change without notice. All efforts have been made to ensure the accuracy of this publication. Notwithstanding, eNitiatives.com Pty. Ltd. does not assume responsibility for any errors nor for any consequences arising from any errors in this publication.

The software and/or databases described in this document are furnished under a licence agreement. The software and/or databases may be used or copied only in accordance with the terms of the agreement.

***ViewDS, ViewDS Access Presence and ViewDS Access Sentinel are trademarks of ViewDS Identity Solutions***

Microsoft is a registered trademark and Windows is a trademark of Microsoft Corporation.

All other product and company names are trademarks or registered trademarks of their respective holders.

# Significant changes in ViewDS 7.4

ViewDS 7.4 has significant changes in the following areas:

- [Licensing](#)
- [Platform support](#)
- [Installation](#)
- [ViewDS server](#)
- [ViewDS Management Agent](#)
- [ViewDS Access Sentinel and the AIKs](#)
- [ViewDS Access Presence](#)
- [Documentation](#)

## Licensing

### New license key system

A new license key system has been introduced in ViewDS 7.4.

As a result of this change you will not be able to use your existing license key when you upgrade from a previous version of ViewDS. Instead you must contact your ViewDS vendor with your old license in order to obtain a replacement. See [Licence requirements](#) for further details.

### Changes to licensing of ViewDS components

We have also reviewed how the various ViewDS components are licensed and as a result only the following ViewDS components now require a license:

- ViewDS server DSA
- ViewDS Access Sentinel
- ViewDS Access Proxy

All other ViewDS components, including the ViewDS Management Agent (VMA) and Access Presence, do not require a license in order to operate.

## Platform support

### Changes to supported platforms in ViewDS 7.4

The following changes have been made to the supported platforms in ViewDS 7.4:

- Support for Sun SPARC Solaris 9 and RedHat Enterprise Linux 4 has been withdrawn
- Support for 64-bit Sun SPARC Solaris 10 and above has been added
- Support for 64-bit RedHat Enterprise Linux 5 and above has been added
- Support for 64-bit Windows Server 2003 and above has been added

### Changes to supported platforms in ViewDS 7.4.5

The following changes have been made to the supported platforms in ViewDS 7.4.5:

- Support for Sun SPARC Solaris and RedHat Enterprise Linux 5 has been withdrawn

See [ViewDS server requirements](#) for full details.

### Future plans

We are reviewing our support for Windows Server 2003, which reached its end-of-life in July 2015. Customers that require continuing Windows Server 2003 support should contact their ViewDS vendor.

We are also reviewing our support for older versions of ViewDS (7.0, 7.1, 7.2 and 7.3) on all platforms. Customers that are still running these older versions should consider upgrading to the latest version of ViewDS as soon as possible. See [Upgrading from a previous version of ViewDS](#) for full details of the upgrade process.

## Scope of release

From ViewDS 7.4.5 onwards we are no longer distributing the Java and .NET AIKs or the IIS and Apache PEPs as part of a standard ViewDS release. Customers that still require these tools should contact their ViewDS vendor to obtain them.

## Installation

A single Windows installer is provided in ViewDS 7.4 that replaces the individual ViewDS Server and ViewDS Management Agent (VMA) installers that were supplied previously.

This installer allows you to install the ViewDS Server and the VMA individually, in much the same way that these ViewDS components were installed in the past. Additionally, the installer enables you to install the ViewDS Server and VMA together on the same Windows machine (and optionally preconfigure the VMA and Access Presence to work with the ViewDS Server). This offers users a quick and easy way to get a new ViewDS instance up and running. See [Installing the ViewDS suite on Windows](#) for further details.

## ViewDS server

### Multi-threading

Significant changes have been made to the ViewDS server to switch from a multi-process architecture to a multi-threaded model. These architectural changes provide immediate performance benefits for existing users.

### Password encryption changes

128 bit AES encryption is now used to protect passwords when they are stored (within the database, log files and dumps) and replicated by ViewDS. AES provides a higher level of security and assurance over DES, which is used by previous versions of ViewDS. The VMA includes an auto-generate feature to assist you with creating the keys required. See the Key Editor window topic in the VMA online help for further details.

As a result of this change it is essential that you know the key used to encrypt passwords in dump files generated by previous versions of ViewDS if you plan to import them into ViewDS 7.4. See [Upgrading from a previous version of ViewDS](#) for full details.

## ViewDS Management Agent

### Usability enhancements in the Global DIT view

New tool and address bars have been added to the Global DIT view in the VMA. The dynamic toolbar provides easy access to common operations such as add/remove access control domain, copy DN, cut/past branch and so on. Previously these operations could only be accessed via a context menu. The address bar allows you to navigate the DIT by typing in a valid DN. See the Global DIT View topic in the VMA online help for full details.

## ViewDS Access Sentinel and the AIKs

### XML Digital Signature support

Access Sentinel can now protect SAML-based XACML access with XML Digital Signature security. XML digital signatures provide mutual strong authentication and data integrity verification for communications between the PEP and the PDP. The X.509 digital certificate that is used to sign XACML requests and/or responses is used by the recipient to perform strong authentication.

Access Sentinel's support for XML digital signatures has been implemented according to the XML Signature Syntax and Processing Second Edition (2008) specification using the methods described in Section 5: SAML and XML Signature Syntax and Processing of the SAML Core Specification 2.0 (2005) with the following variation:

- The KeyInfo element is always included in a signed response and contains either the X509Certificate or the X509SubjectName.

See the ViewDS Technical Reference Guide: Directory System Agent for full details.

### XACML REST profile support

Access Sentinel now supports the REST Profile of XACML v3.0, Version 1 OASIS standard, allowing any external applications that also support this standard to interact with Access Sentinel for authorization decisions.

The implementation allows the use of XACML in a RESTful architecture, enabling interoperability of RESTful Authorization-as-a-Service (AZaaS) solutions. Unlike the SAML profile, this method does not require the use of SOAP and allows XML-based authorization requests and responses to be transported directly over HTTP.

### XACML JSON over REST support

Access Sentinel now supports the Request / Response Interface based on JSON and HTTP for XACML 3.0, Version 1.0 (Working Draft 14) OASIS draft standard, allowing any external applications that also support this draft standard to interact with Access Sentinel for authorization decisions.

The implementation allows the use of JSON to represent authorization request and response messages that are sent via REST.

## Resource attribute lookup

Access Sentinel is now able to look-up resource attributes when evaluating external authorization requests. This ability to locate the resource entry provides two benefits:

- Attributes for a particular resource can be obtained and used when evaluating authorization decisions.
- Locating the resource entry allows Access Sentinel to determine if the resource falls within the scope of the target for a given policy.

## Access Sentinel Administrative Interface renamed Authorization Policy Manager

The Java-based Policy Administration Point (PAP) application included with Access Sentinel, previously known as the Access Sentinel Administrative Interface, is now called the Authorization Policy Manager.

## AIK support for signing requests and verifying signed requests

Both AIKs now support XML Digital Signature security. Authorization requests can be signed before they are sent to the server using the `XmlSigningConnector` object and signed requests can be verified for all connector objects. See the Simple authorization requests topics for [Java](#) and [.NET](#) for further details.

## AIK support for REST and JSON

Both AIKs now support the communication methods JSON over REST and XML over REST, in addition to XML over SOAP, for communication with the PDP. See the Simple authorization requests topics for [Java](#) and [.NET](#) for further details.

## AIK support for HTTPS connections to server

Both AIKs are now able to send authorization requests over a secure HTTPS connection using the `ClientSslConnector` object. See the Requests over a secure connection topics for [Java](#) and [.NET](#) for further details.

## AIK support for multi-requests and responses

Both AIKs now allow you to combine multiple authorization requests into a single multi-request object. This object is then sent to the PDP, which returns a multi-response object. See the [Multiple requests](#) topic for full details.

## AIK support for Trace information

Both AIKs now provide a tracing feature that allows you to investigate the cause of any unexpected responses obtained from the PDP. See the [Tracing](#) topic for full details.

## AIK support for arbitrary XML content to be included in requests

Both AIKs now support the content element for attributes in a request. This means that requests can now include a free-form XML document within a given category to represent the Resource, Subject, Action or Environment.

## ViewDS Access Presence

### Annotated types

Annotated forms of three primitive types have been added to Access Presence:

- AnnotatedOctetString
- AnnotatedDistinguishedName
- AnnotatedUTF8String

These enable you to add annotations to attribute values of matching types. For example, you could define an image attribute using the AnnotatedOctetString type. This attribute would allow you to store images and associate an annotation with each image. The annotation could be the alternative text used in the HTML <img> tag or the MIME type to be used when processing the image. See the ViewDS Technical Reference Guide: User Interfaces for full details.

### Ability to manage individual values of an attribute

Access Presence now allows you to modify individual values of a multi-value attribute. In the case of images, for example, this feature enables you to manage one binary image file separately from other image values. See the ViewDS Technical Reference Guide: User Interfaces for full details.

### att.mime file format changes

The format of the MIME mapping file, att.mime, has been modified to allow the components of a complex attribute value (such as an annotated type) to be identified. The content type field can also use the "%{}" syntax (already used in the content disposition field) to obtain the content from a component of complex value. For example, you could use the att.mime file to display an image and use its annotation to control the MIME type with the following :

```
image.value ${annotation}
```

Where `image.value` identifies the where the binary image is held and `${annotation}` indicates that the annotation should be used as the MIME type.

See the ViewDS Technical Reference Guide: User Interfaces for full details.

### Ability to define presentation rules for components of a complex attribute

In order to provide control over the presentation of the fields in complex attribute values, the attribute presentation has been extended to allow information about fields to be provided. This information is used on the modify value form and the expanded entry form.

Presentation rules, such as a drop down list of values, can be associated with a particular component of a complex value, like the annotation field. For example, if you are maintaining annotated images, you might wish to provide a enumerated list of values to choose from when specifying the MIME type.

See the ViewDS Technical Reference Guide: User Interfaces for full details.

## Documentation

The following ViewDS documents are now available in a fully searchable webhelp format online at [www.viewds.com/documentation/viewds/](http://www.viewds.com/documentation/viewds/):

- ViewDS 7.4 Release Notes
- ViewDS Installation and Operations Guide
- ViewDS Access Proxy Installation Guide
- ViewDS Access Sentinel Installation and Reference Guide
- ViewDS Application Integration Kit for .NET
- ViewDS Application Integration Kit for Java

In addition, software reference documents for both the .NET and Java AIKs are available online at [www.viewds.com/resources/documentation.html](http://www.viewds.com/resources/documentation.html).

# All changes in ViewDS 7.4 Patch 1

This section lists all the changes and issues resolved in ViewDS 7.4 Patch 1.

## Documentation

**VIEWDS-633:** The description of how the XACML policy combining algorithm is used by Access Sentinel that was provided in the ViewDS Installation and Operations guide and in the VMA help was misleading. This has been resolved.

## ViewDS Suite Installer

**VIEWDS-829:** Previously the ViewDS Suite Installer added a server connection automatically when only the VMA was being installed. This has been resolved.

**VIEWDS-856:** Previously the ViewDS Suite Installer installed some unnecessary IIS components. This has been resolved.

## ViewDS Management Agent

**VIEWDS-713:** After performing a quick search, the keyword used now appears only once in the recent searches list.

**VIEWDS-751:** The VMA now reports when imported structure rules are ignored.

**VIEWDS-787:** References to "Web DUA" - the old name for Access Presence - have now been removed from the VMA.

**VIEWDS-789:** It is now possible to convert a shadow plane to a master plane using the VMA. See the VMA help topic *Local DIT tab - Shadow tab* for further details.

**VIEWDS-795:** The old icons displayed in the context menu for DIT entires have been replaced with the latest versions.

**VIEWDS-803:** Toolbar icons in the Global DIT View are now refreshed correctly after adding or removing an access control domain or a subschema access point.

**VIEWDS-809:** Problems with the display of the Global DIT View when only the RAS is connected have been resolved.

**VIEWDS-810:** A spurious error about the format of valid DateTime values displayed when modifying Attribute Presentation attributes using the VMA has been eliminated.

**VIEWDS-812:** It is now possible to modify an existing certificate proxy.

**VIEWDS-814:** It is now possible to replace a condition in the XACML Expression editor before specifying a value.

**VIEWDS-832:** Problems with the display of the Global DIT View when a new license key is added have been resolved.

**VIEWDS-833:** A spelling mistake in an installer message displayed when attempting to add a connection to a local DSA that is already connected has been corrected.

**VIEWDS-836:** The VMA no longer reports a constraint violation error when an XACML expression is saved as a rule condition.

## Directory Service Agent

**VIEWDS-715:** An XACML access control domain split across a superior and a subordinate DSA will no longer deadlock.

**VIEWDS-738:** The OpenSSL libraries used by ViewDS have been updated to version 1.0.1j.

**VIEWDS-782:** Failures when replicating very large databases with over 150 million entries have been resolved.

**VIEWDS-784:** Excessive memory and time consumption issues when replicating very large databases have been resolved.

**VIEWDS-786:** Previously input/output conflicts could occur when a shadow plane was removed. This has been resolved.

**VIEWDS-790:** Previously using LDAP to make changes to indexes could result in the indexes not being rebuilt immediately. This has been resolved.

**VIEWDS-794:** SunDS passwords can now be loaded into and evaluated by ViewDS. See the ViewDS Technical Reference Guide: Directory Service Agent for further details.

**VIEWDS-796:** It is now possible to add a knowledge reference to a master on a shadow instance after replication has been enabled without obtaining errors.

**VIEWDS-813:** Previously, chaining to LDAP or non-OSI directories could result in unnecessary operation timeouts. This issue has been resolved.

**VIEWDS-845:** The dsasrv process no longer terminates unexpectedly when handling high loads.

**VIEWDS-851:** Previously the DSA maintained internal references to context prefixes incorrectly. This has been resolved.

**VIEWDS-852:** The DSA has been modified and now ignores the Manage DSA IT LDAP Control when it is being misused by clients.

## Access Presence

**VIEWDS-716:** Enhancements have been made to the security of Access Presence cookies. See *Access Presence Cookies* in the ViewDS Technical Reference Guide: User Interfaces for further details.

**VIEWDS-743:** It is now possible to format the first entry in a search results list differently from the other entries in the list. See the ViewDS Technical Reference Guide: User Interfaces for further details.

## Access Sentinel

**VIEWDS-785:** The Apache PEP now handles SAML responses returned by Access Sentinel.

# All changes in ViewDS 7.4 Patch 2

This section lists all the changes and issues resolved in ViewDS 7.4 Patch 2.

## Documentation

**VIEWDS-945:** The XACML example in the [Declare XACML attributes](#) topic contained an error that caused it to fail. This has been resolved.

## ViewDS Suite Installer

**VIEWDS-865:** Previously the ViewDS Suite Installer did not remove the VFHOME variable when uninstalling. This has been resolved.

## ViewDS Management Agent

**VIEWDS-869:** Problems with the show/hide behaviour of items in the View menu have been resolved.

**VIEWDS-876:** Previously the VMA would terminate unexpectedly if users attempted to display an entry in the DIT that was obscured due to the specified Maximum number of subordinate entries having been exceeded. This has been resolved.

**VIEWDS-880:** When a DSA cannot be started by the RAS, an administrator will have to rectify the underlying problem before attempting another restart. Sometimes this may involve replacing a license key which has become invalid. Previously, the VMA exhibited a problem that prevented the DSA from being re-started through the VMA in such circumstances. This has been resolved. Additionally, a visual indicator has been added to the Server Graphical View that shows when a valid licence is absent.

**VIEWDS-896:** Previously, users may have experienced problems with the VMA crashing or becoming unresponsive and consuming large amounts of CPU resources when attempting to manage the subordinate object classes within the presentation rules for an object class. This has been resolved..

## Directory Service Agent

**VIEWDS-351:** To resolve interoperability problems with some LDAP tools, the DSA now accepts the SSLv2 and SSLv3 client hello messages. It will not allow SSLv2 or SSLv3 to be used to secure a connection, but will allow the initial messages from a client to use these protocols to initiate a connection.

**VIEWDS-701:** To prevent 64bit dsasrv processes causing memory exhaustion, a new dsac setting called heapsize has been added. This specifies the combined amount of heap memory that the DOTs are permitted to have allocated at any time. Operations that try to go over the specified heap size limit will be aborted. See the VMA help topic Configuration tab - Runtime Settings or the ViewDS Technical Reference Guide: Directory System Agent for more details.

**VIEWDS-875:** Previously, searches of large (1 million plus entry) databases could fail when indexes were being rebuilt. This has been resolved.

**VIEWDS-878:** Previously, a one time failure might be observed when performing a search directly after moving a context prefix entry. This issue was caused by an outdated search result persisting in the internal cache. It has been resolved.

**VIEWDS-879:** Previously, an internal failure might be observed when performing a rename operation on a recently moved context prefix entry. The internal issue that caused this problem has been resolved.

**VIEWDS-905:** When a context prefix entry is moved below another master entry, it should no longer be a context prefix. ViewDS was failing to make this reassessment. This has been resolved.

**VIEWDS-911:** Previously, ViewDS would not evaluate IPv4 based licenses against all IPv4 addresses on the host server. This has been resolved.

**VIEWDS-913:** An internal error no longer occurs when adding a directory attribute value using LDAP that conforms to an XML schema in which an element has an undefined XML attribute that is permitted by an <anyAttribute> definition.

**VIEWDS-916:** Spurious carriage returns in SDUA output on Windows have been eliminated.

**VIEWDS-917:** Previously an invalid schema might cause VFLOAD to fail. This has been resolved.

**VIEWDS-933:** Problems with re-opening the ViewDS server database after it has been closed have been resolved.

**VIEWDS-935:** A new RAS command to send SIGKILL signal to DSA service has been added.

**VIEWDS-940:** The SASL DIGEST-MD5 authentication mechanism is now working properly.

## Access Sentinel

**VIEWDS-895:** Both the Java and .NET AIKs now provide an appropriate exception message when the XACML extension is null.

**VIEWDS-921:** A problem which prevented the .NET AIK from sending JSON\_REST MultiRequests has been resolved.

**VIEWDS-924:** The Java AIK now provides appropriate exception messages when JSON\_REST is used with unsupported flags and connector types.

**VIEWDS-925:** The Java AIK now checks that a signing keypair is supplied for XmlSigningConnector and provides an appropriate exception message if it is not.

**VIEWDS-926:** The .NET AIK now checks that a client ssl certificate is supplied for ClientSslConnector and provides an appropriate exception message if it is not.

**VIEWDS-937:** Previously, double quotes were erroneously stored as part of the AttributeAssignment value when the JSON\_REST communication type was used in Java AIK. This has been resolved.

# All changes in ViewDS 7.4 Patch 3

This section lists all the improvements and issues resolved in ViewDS 7.4 Patch 3.

## ViewDS Suite Installer

### New features

**VIEWDS-1069:** The ViewDS suite Installer can now be used to install the ViewDS Directory Server, VMA and Access Presence on Windows 10.

### Bug fixes

**VIEWDS-1004:** Previously, if the ViewDS suite Installer failed to complete the installation process for any reason, then it did not stop or delete the RAS service during rollback. This has been resolved.

## ViewDS Management Agent

### New features

**VIEWDS-977:** The VMA now reports detailed information about the status of each DOT thread in the Server View on the Status - General tab (Text View).

**VIEWDS-968:** The number of pending replication operations is now displayed in the Server View on the Replication tab for Supplier Agreements.

### Bug fixes

**VIEWDS-883:** Previously it was not possible to convert a shadow to a master if the VMA was connected to the consumer DSA using the same certificate as the supplier DSA. Additional checks have been implemented to allow this in most circumstances.

**VIEWDS-964:** A problem which caused the VMA to become unresponsive if a user navigated away from a window while a table was being populated with data has been resolved.

**VIEWDS-974:** It is not possible to edit the components of the CertificatePair attribute properly using the VMA. A file import mechanism has been implemented to resolve this issue.

**VIEWDS-990:** Previously, the VMA listed both indexed attributes and attributes with extensions in the Global DIT View on the Schema - Indexing - Attribute Indexing tab. Now, only indexed attributes are displayed.

**VIEWDS-994:** Problems with the auto-adjust column width feature in the Server View on the Replication tab have been resolved.

**VIEWDS-1043:** The VMA now recognises and therefore allows users to add attributes with PFX syntax.

## Directory Service Agent

### New features

**VIEWDS-966:** The number of pending replication operations can now be obtained from the `supplierStatus` attribute.

**VIEWDS-979:** Status messages have been added to the error log to report when processing of a coordinate or update shadow operation starts and finishes at both the initiating and responding DSAs.

**VIEWDS-995:** Strong authentication now supports certificates signed using the SHA2 algorithm.

**VIEWDS-1011:** An optional configurable threshold has been added to the `supplierStatus` attribute to automatically trigger a total refresh if the number of incremental updates exceeds the threshold. See *triggerTotalRefresh* in *Chapter 7* of the ViewDS Technical Reference Guide: Directory Service Agent for further details.

**VIEWDS-1017:** A new operational attribute has been added that publishes attribute type definitions using LDAP-specific encoding of the `AttributeTypeDescription` syntax. See *ViewDS-specific operational attributes* in *Appendix B* of the ViewDS Technical Reference Guide: Directory Service Agent for further details.

**VIEWDS-1021:** UTF8String values can now be loaded from a file using the Stream DUA.

**VIEWDS-1026:** LDAP password management support has been extended to provide a mechanism for locking accounts after they have been inactive for a configurable period of time. See *LDAP password management* in *Chapter 6* of the ViewDS Technical Reference Guide: Directory Service Agent for further details.

**VIEWDS-1028:** LDAP password management has been augmented with two new ViewDS specific operational attributes that:

- identify the set of password quality checks that are carried out if the pwdCheckSyntax behaviour is enabled.
- perform a password distance check if the pwdCheckSyntax behaviour is enabled. This imposes a minimum degree of change between old and new passwords and so prevents the use of sequential passwords.

See *ViewDS-specific password policy operational attributes* in *Chapter 6* of the ViewDS Technical Reference Guide: Directory Service Agent for further details.

## Bug fixes

**VIEWDS-915:** XPath expressions involving the special values NaN, INF or -INF were returning the wrong results on Windows. This has been resolved.

**VIEWDS-916:** The Stream DUA catalog strings contained spurious carriage return characters on Windows. This has been resolved.

**VIEWDS-955:** The value of Max. Heap Size was being reset to the default after the DSA was restarted. Now any user defined value provided is retained after the DSA is restarted.

**VIEWDS-999:** Status messages about ignoring the userPassword attribute when LDAP requests for user attributes are being processed have been removed from the error log, as they added little value and were occurring frequently.

**VIEWDS-1000:** Search operations on a shadow DSA were being chained to the master DSA unnecessarily. This has been resolved.

**VIEWDS-1001:** Previously, all replication agreements would hang if any connection attempt from the supplier DSA to a consumer was improperly established. A new configurable timeout limit for connection attempts has been added to abort such connections attempts and allow other connected replication agreements to be processed.

**VIEWDS-1005:** Previously the RAS process was using a lot of memory when it was monitored continuously by VMA. This has been resolved.

**VIEWDS-1060:** The timestamp of the last failed bind or compare operation was not being recorded correctly in the pwdFailureTime attribute when password policy was enabled. This has been resolved.

## Access Presence

### New features

**VIEWDS-1025:** Password policy can now be enforced through Access Presence. See *webUsePasswordPolicy* in the ViewDS Technical Reference Guide: User Interfaces for further details.

### Bug fixes

**VIEWDS-992:** Previously users were unable to change their passwords using the *newpassword* template if directory-based session management was enabled. This has been resolved.

**VIEWDS-1055:** Previously, the Access Presence form for modifying individual values presented Boolean values in string form but did not accept this string form as valid input. This has been resolved.

## Access Sentinel

### Bug fixes

**VIEWDS-941:** Previously it was not possible to send XMLContent using MultiRequest in the .NET AIK. This has been resolved.

**VIEWDS-942:** Previously, when XMLContent with the same CategoryId appeared in more than one request, the resulting MultiRequest would only recognise the XMLContent in the first request and ignore the remaining XMLContent. This has been resolved.

# All changes in ViewDS 7.4 Patch 4

This section lists all the improvements and issues resolved in ViewDS 7.4 Patch 4.

## ViewDS Management Agent

### Bug fixes

**VIEWDS-1102:** Previously an error occurred when viewing the Rules tab on the Object Class Properties window if the optional name field for a rule was unpopulated. This has been resolved.

## Directory Service Agent

### New features

**VIEWDS-1092:** In order to make it easier to identify slow and long running searches, the duration of each operation is now recorded in the ViewDS query and update logs.

The duration of an operation is recorded in the query and update logs at the end of the first line of the preamble. The time is reported in seconds. For example:

```
# 1450323661 8 DAP Thu Dec 17 14:41:20 2015 duration 0.698
# performed by (osi://localhost:51901)
search {
}
for
    objectClass present
options {
    serviceControls {
        timeLimit 5
    }
}
;
```

The duration of the operation is recorded from when a DOT receives the operation to when it logs the operation. This includes only the time for however many transactions are required to complete the operation

(generally only updates require more than one transaction). It does not include the time the operation was queued awaiting a DOT.

## Bug fixes

**VIEWDS-1114:** Previously the DSA would hang when attempting to make schema changes using a VMA located on the same server as the DSA under Windows Server 2008 R2. This was due to the state of the dot state machine in the dsasrv thread not being reset to the correct settings before a new operation was assigned to the dot. This problem has been resolved.

**VIEWDS-1126:** Previously indexing corruption issues would occur when making changes to schema. This was due to inconsistencies in the way the keyword synonym index was maintained. This problem has been resolved.

## Access Presence

### New features

**VIEWDS-1086:** Enhancements have been made to prevent cross-site request forgery.

A nonce has been added to the session object that is included and verified in all URLs, except for some specific query URLs that might be bookmarked, such as search results pages and expanded entry forms.

**VIEWDS-1087:** It is now possible to delete multiple entries in a single operation in Access Presence.

A new form called Select Entries to Remove has been added to select the entries in the target object cache to remove from the directory. See *Access Presence templates* in the ViewDS Technical Reference Guide: User Interfaces for further details.

### Bug fixes

**VIEWDS-934:** Previously, the mandatory naming attribute commonName did not appear on Modify form when only add permission was set for a user. This had been resolved.

**VIEWDS-1002:** Previously, invalid values for attributes of INTEGER syntax with trailing non-numeric characters were accepted on the Modify form. This has been resolved.

**VIEWDS-1111:** Previously a number of the default Access Presence templates could not be used by anonymous users. This has been resolved.

**VIEWDS-1117:** The <VFAssPassTable> template tag, which allows you to modify both the privilege and userEntitlement attributes on the Assign Password form, was not presenting userEntitlement attributes when no values were already present for those attributes. This problem has been resolved.

**VIEWDS-1124:** Previously, when Access Presence was being used to update entries through a shadow DSA, any attributes with reverse links configured caused errors to be reported in Access Presence even though the updates appeared to work correctly. This was due to information from the shadow DSA being used to decide what changes were required to maintain the reverse links rather than chaining these query operations to the master. This problem has been resolved.

**VIEWDS-1139:** Previously, an error was returned when attempting to print reports with HTTP sessions enabled. This was due to the pdua program being invoked using anonymous credentials. This problem has been resolved.

**VIEWDS-1142:** Previously an error might be returned when attempting to set context on the Search form with HTTP sessions enabled. This problem has been resolved.

# All changes in ViewDS 7.4 Patch 5

This section lists all the changes, improvements and issues resolved in ViewDS 7.4 Patch 5.

## Platform support

### Changes to supported platforms

The following changes have been made to the supported platforms with this release:

- Support for Sun SPARC Solaris has been withdrawn
- Support for RedHat Enterprise Linux 5 has been withdrawn

See [ViewDS server requirements](#) for full details.

### Future plans

We are reviewing our support for older versions of ViewDS (7.0, 7.1, 7.2 and 7.3) on all platforms. Customers that are still running these older versions should consider upgrading to the latest version of ViewDS as soon as possible. See [Upgrading from a previous version of ViewDS](#) for full details of the upgrade process.

## Scope of release

We are no longer distributing the Java and .NET AIKs or the IIS and Apache PEPs as part of a standard ViewDS release. Customers that still require these tools should contact their ViewDS vendor to obtain them.

## Directory Service Agent

### New features

**VIEWDS-1138:** The OpenSSL libraries used by ViewDS have been updated to version 1.1.0f.

**VIEWDS-1178:** Caching of paged results for LDAP, XLDAP, DAP search and DAP list has been implemented. This has been done to improve search speeds.

The paged results are stored as files in the `$VFHOME/tmp` (`tmpdir`) directory. A new config file option, `pagedresultcachesize`, has been added to control how many outstanding paged results are kept. This is an integer with a default value of 6.

A paged result is discarded to free up a slot in the cache, when the last page is returned or when the client explicitly abandons the request.

See the ViewDS Technical Reference Guide: Directory Service Agent for further details.

## Bug fixes

**VIEWDS-1146:** Previously, a problem in our transport layer implementation, resulted in us sending transport protocol data units (TPDUs) that were larger than the negotiated size because we were not including the TPDU header in the length restriction. The problem only showed up if the session layer did not negotiate a transport service data unit (TSDU) size. To resolve the issue the TSDU size used should now always be smaller than the TPDU size, to allow for the TPDU header to be included in the negotiated TPDU size.

**VIEWDS-1150:** The `-d` command line option to `sdua` is used to include the `manageDSAIT` service control option in DAP requests and the `manageDSAIT` LDAP control in LDAP requests. However, since LDAP password policy support was made accessible in DAP, the `-d` option was incorrectly adding the LDAP `manageDSAIT` control to DAP requests in addition to the service control option. This has now been fixed.

**VIEWDS-1161:** Previously, an XBAC expression comparing a subject entryUUID to a resource entryUUID would fail. The subject attribute lookup procedure in the PDP was right. However, the resource attribute lookup procedure was assuming that resource attributes are always user attributes, whereas entryUUID is an operational attribute, so the lookup returned an empty bag. This has now been resolved.

**VIEWDS-1162:** Previously, the XBAC internal PEP was not properly initialising an attribute value with integer syntax, leading to an internal error and an `unwillingToPerform` response. This has now been fixed.

**VIEWDS-1169:** Previously, the time field provided by `sdua` in a strong authentication bind token used second resolution. This could cause bind failures when the resolution was not fine enough for the frequency at which the bind operations were occurring. The resolution of the time field in the `sdua` bind token has been increased to millisecond to address this.

**VIEWDS-1170:** Previously, parsing of an XACML authorization request in JSON format with an array of values of the `xpathExpression` data-type failed with an Indeterminate result. This has now been resolved.

**VIEWDS-1175:** Previously, XACML request durations were not being recorded accurately in the query log. This has now been fixed.

**VIEWDS-1196:** Previously, valid JSON-format XACML requests were occasionally rejected with the spurious error `double value is not representable`. This has now been resolved.

**VIEWDS-1255:** Previously, the XACML time functions `time-equals`, `time-less-than`, `time-less-than-or-equal-to`, `time-greater-than`, `time-greater-than-or-equal-to` and `time-in-range` did not necessarily give the correct results with time values that included a time zone. This has now been fixed.

## Access Presence

### New features

**VIEWDS-1100:** Access Presence now supports authenticator devices that provide time-based one time passwords, such as Google Authenticator. These new configuration file options have been added to control this behaviour:

- `websessionauthenticator` - String value containing the name of an attribute in which the authenticator secret is stored in the user's entry.
- `webauthenticatortemplate` - String value containing the path name of the HTML template file for presenting the page requesting the authenticator code from the user.
- `webisableauthenticatortemplate` - String value containing the path name of the HTML template file for presenting the page for disabling an authenticator for the current user.
- `webenableauthenticatortemplate` - String value containing the path name of the HTML template file for presenting the page for enabling an authenticator for the current user.

In addition a number of new Access Presence template tags have been added to control the format of the authenticator page. See the ViewDS Technical Reference Guide: User Interfaces for full details.

**VIEWDS-1153:** Access Presence now supports the SAML2 Web SSO profile, acting as the service provider. These new configuration file options have been added to control this behaviour:

- `websamlentity` - String value containing the URI use to identify the WebDUA service provider entity.
- `websamlendpoint` - String value containing an optional callback URL for Access Presence, to be included in SAML2 authentication requests made by Access Presence.
- `websamlidpurl` - String value containing the URL of the SAML2 identity provider authentication endpoint.

- `websamltrustanchor` - String value containing the name of the certificate that Access Presence should use to verify the signature on the SAML assertions provided by the SAML2 identity provider.

This implementation uses the HTTP Redirect binding for SAML authentication requests and expects the SAML response to be provided using the HTTP Post binding. At present, only the X.509 Certificate representation of public key information in the XML signature is supported.

Access Presence expects an identity to be provided in the NameID element of the SAML2 assertion's Subject element. It will map the NameID to an identity in the directory using the attribute identified by the `web-proxyauthattribute` configuration file option.

See the ViewDS Technical Reference Guide: User Interfaces for full details.

## Bug fixes

**VIEWDS-1160:** Previously, searches by anonymous users on Access Presence sites set-up for both Proxy Authorisation and anonymous access would fail. This has now been resolved.

**VIEWDS-1168:** Previously, the reports template required a nonce, which was included in the URL generated by `VFPrintFormHref`. This caused an `Invalid nonce provided` error when accessed by an anonymous user on a system where sessions were enabled. This has now been fixed.

# Issues when upgrading to ViewDS 7.4

The following must be considered when upgrading to ViewDS 7.4.

## Licensing changes

A new license key system has been introduced in ViewDS 7.4.

As a result of this change you will not be able to use your existing license key when you upgrade from a previous version of ViewDS. Instead you must contact your ViewDS vendor with your old license in order to obtain a replacement. See [Licence requirements](#) for further details.

## Password encryption changes

128 bit AES encryption is now used to protect passwords when they are stored (within the database, log files and dumps) and replicated by ViewDS. AES provides a higher level of security and assurance over DES, which is used by previous versions of ViewDS. The VMA includes an auto-generate feature to assist you with creating the keys required. See the Key Editor window topic in the VMA online help for further details.

As a result of this change it is essential that you know the key used to encrypt passwords in dump files generated by previous versions of ViewDS if you plan to import them into ViewDS 7.4. This key is available through the ViewDS Management Agent, on the **Configuration** tab in the **Runtime Settings** pane. If no key is included on the **Runtime Settings** pane, then the default ViewDS key - MePh2P - is used. You will need this key when loading the dumped files into ViewDS 7.4. See [Upgrading from a previous version of ViewDS](#) for full details.

# Known Issues

Below is a summary of the known issues and limitations in ViewDS 7.4 Patch 4.

## ViewDS suite Windows installer unable to install IIS on Windows 10

### Issue

The ViewDS suite installer for Windows fails if Access Presence is installed on a Windows 10 machine which does not already have IIS installed on it.

### Workaround

It is possible to overcome this problem by either deselecting Access Presence when the installer provides that option or installing IIS prior to launching the ViewDS installer. To do this:

- Click Start and start to type "Turn Windows features on or off".
- Select **Turn Windows features on or off** from the list of search results. The **Windows Features** dialog is displayed.
- Check **Internet Information Services**.
- Check **Internet Information Services > World Wide Web Services > Application Development Features > CGI**.
- Click **OK** to install both modules.
- Click **Close** to dismiss the **Windows Features** dialog when the installation is complete.

## Password guessing limits are not enforced by Access Presence in certain circumstances

### Issue

The password policy `pwdFailureTime` attribute is not updated for failed Access Presence login attempts when cookie-based session management is used. As a result, any policy defined by the `pwdMaxFailure` attribute will not be enforced in these circumstances.

## Workaround

Enable directory-based session management. See *Directory-based Session Management* in *Chapter 2* of the ViewDS Technical Reference Guide: User Interfaces for further details.

## A Windows Application Error dialog is presented when the DSA terminates unexpectedly preventing the RAS from restarting the DSA

### Issue

In general, if the DSA process terminates unexpectedly, the RAS service will detect this and restart the DSA. However, in certain circumstances beyond our control, the Windows operating system displays a dialog which reports that a problem has occurred with the DSA process. When this happens, the DSA process is not properly terminated and cannot be restarted by the RAS until someone interacts with the dialog and closes it. This can result in undesirable downtime.

### Workaround

Locating and closing the Windows Application Error dialog allows the DSA process to terminate properly and the RAS to restart the DSA.

However, if this problem is causing issues regularly, you may wish to familiarise yourself with the Windows Error Reporting ([https://msdn.microsoft.com/en-us/library/bb513641\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/bb513641(v=vs.85).aspx)) system and investigate the `dontShowUI` setting ([https://msdn.microsoft.com/en-us/library/bb513638\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/bb513638(v=vs.85).aspx)) which will disable the user interface dialog.

These settings apply to the entire operating system, not just ViewDS, and therefore it is important to understand the wider impact of and be cautious when making any changes.

## ViewDS suite Windows installer crashes occasionally

### Issue

The ViewDS suite installer for Windows occasionally reports the following error at installation time:

The application ran into a problem that it couldn't handle.  
Sorry for the inconvenience.

This error is generated by the third party installer software with which the ViewDS suite installer is built.

### **Workaround**

It is possible to overcome this problem by re-running the installer.

## **ViewDS suite Windows installer may fail when installing Access Presence on Windows Server 2003**

### **Issue**

The ViewDS suite installer for Windows fails if Access Presence is installed on a Windows Server 2003 machine which does not already have IIS installed on it.

### **Workaround**

It is possible to overcome this problem by either deselecting Access Presence when the installer provides that option or installing IIS prior to launching the ViewDS installer.