ViewDS Version 7.5

Release Notes

Published: 2020
Version: 7.5

ViewDS Version 7.5 Release Notes

August 2020

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

ABN 19 092 422 47

Contents

Introduction

These release notes provide information specific to ViewDS Version 7.5.

For information about how to install and use ViewDS see the *ViewDS Installation and Operation Guide* and the *ViewDS Management Agent help*.

This document includes the following:

- Significant changes in ViewDS 7.5
- All changes in ViewDS 7.5
- Bug fixes
- Known issues

Significant changes in ViewDS 7.5

ViewDS 7.5 has significant changes in the following areas:

- ViewDS Windows installers
- Import and export XACML policy
- Composition-time XACML delegation
- XACML policy precedence
- Authorization Policy Manager: Trusted mode
- XACML role enablement
- VMA Settings window
- VMA error log
- CORS support

ViewDS Windows installers

In addition to the ViewDS Suite installer for Windows, this release also includes a dedicated installer for the ViewDS Management Agent (VMA):

- *ViewDS Suite installer* – allows you to select one or more of the following to be installed on the same computer: VMA, ViewDS server, Access Presence. The default install location is '`/Program Files/ViewDS Suite`'.
- *ViewDS VMA installer* – allows you to install the VMA locally (interactive mode) or to a remote computer (unattended mode). The default install location is '`/Program Files/ViewDS`'.

Installing or removing one package has no effect on the other.

Both installers require:

- 32 or 64-bit Windows 7 or later; or
- 32 or 64-bit Windows Server 2008 R2 or later

When installing the VMA, the following requirements also apply.

VMA installation requirements

The VMA requires Microsoft .NET Framework Version 3.5 SP1.

When installing the VMA on a Windows 10 host:

- .NET Framework 3.5 SP1 is installed with Windows 10 by default, but must be enabled before installing the VMA. You can do this through the Windows Features area of the host's Control Panel, or by granting 'Install Windows Features' access to the host's user.

Otherwise, for a non Windows 10 host:

- If not already installed, the VMA installer will install and enable the .NET Framework 3.5 SP1 on the host.

The VMA is only compatible with ViewDS server version 7.5 or above.

Installation modes

The ViewDS VMA installer has two modes: **interactive** and **unattended**. The unattended mode allows you to complete a remote installation through the likes of Active Directory GPO.

The main difference between the modes is that interactive mode installs default PKI certificates.

The ViewDS VMA installer also provides the option to generate an installation log.

Import and export XACML policy

The ViewDS Management Agent (VMA) and Authorization Policy Manager allow you to import and export XACML policy.

The Import Policy Wizard is available from the following tabs (within the XACML AC tab) and is context sensitive:

- Policy Versions tab - open the wizard from this tab to import an entire XACML policy, or one or more of its elements (rules, named expressions, XACML attributes, roles).
- Attributes tab - open the wizard from this tab to import XACML attributes.
- Roles tab - open the wizard from this tab to import roles.

The Policy Versions tab also provides the option to export XACML policy to a file.

Composition-time XACML delegation

XACML policy has two broad categories:

- Access policy, which declares rules that determine whether Access Sentinel grants or denies access to a resource.
- Administrative policy, which declares rules that authorize access policies.

Access Sentinel ignores an access policy unless:

- it was written by an administrator; or
- it is authorized by a chain of administrative policies, where the final policy of the chain was written by an administrator.

The policy is then deemed ‘trusted’.

Only an administrator can manage trusted policies. An administrator is a trusted user of the Authorization Policy Manager or ViewDS Management Agent.

However, an administrator can delegate authorization to manage trusted policy. The administration of policies can therefore be decentralised by delegating trust to users of the Authorization Policy Manager.

Access Sentinel’s XACML framework provides two ways to delegate trust:

- Evaluation-time delegation
- Composition-time delegation

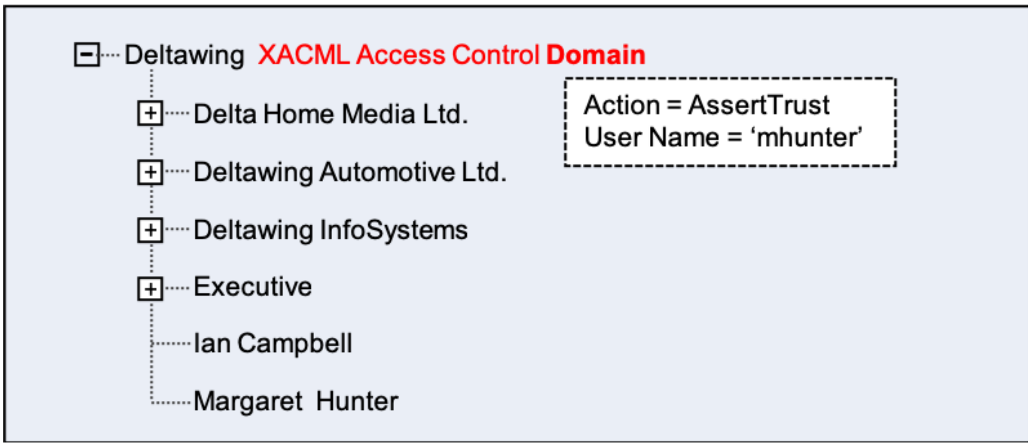
The second option is new to this release of ViewDS.

With composition-time delegation, an administrator can create an access policy that delegates administrator rights within an *XACML Access Control Domain* or within an *XACML Access Control Subdomain*.

Each option is described below.

XACML Access Control Domain

To illustrate composition-time delegation within a domain, consider the following illustration.



Action = AssertTrust
User Name = ‘mhunter’

In this example an administrator has created:

- an *XACML Access Control Domain* at the Deltawing entry

And written an access policy that:

- delegates trust by permitting the action ‘AssertTrust’ by a non-administrative user, Margaret Hunter

Consequently, after starting the Authorization Policy Manager in trusted mode, Margaret Hunter would be able to manage policy within the XACML Access Control Domain.

There would, however, be no restrictions on the non-administrative user. Margaret Hunter would be able to modify every aspect of the access controls in the domain: rules, attributes, versions, policies, roles, and named expressions.

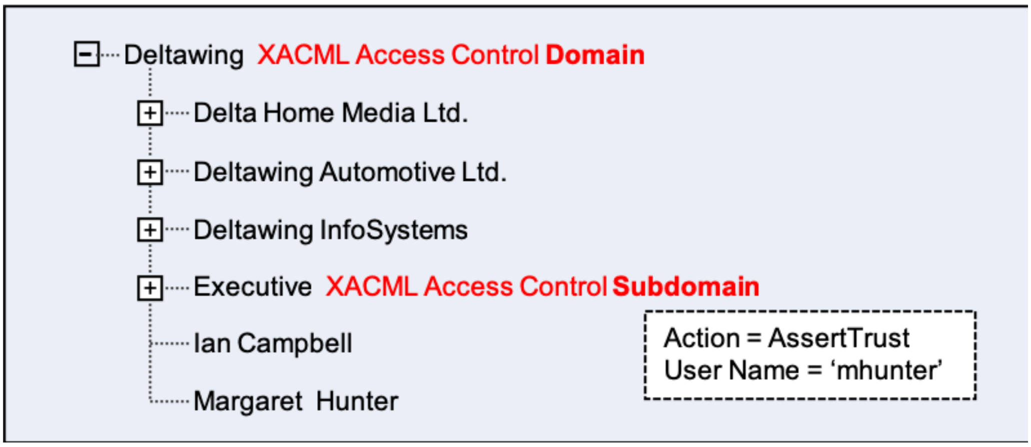
The only way to impose a restriction would be to use precedence. For example, the administrator could amend the access policy so that the non-administrative user can only manage policy containing rules with a precedence greater than 1.

Therefore, a rule with a precedence of 0 or 1 could only be modified by an administrator, and would always override those managed by the non-administrative user.

This restriction would only apply to a policy's rule as attributes, versions, roles and named expressions cannot be assigned a precedence.

XACML Access Control Subdomain

To illustrate composition-time delegation within a subdomain, consider the following illustration.



⊟ Deltawing XACML Access Control **Domain**

⊞ Delta Home Media Ltd.

⊞ Deltawing Automotive Ltd.

⊞ Deltawing InfoSystems

⊞ Executive XACML Access Control **Subdomain**

Ian Campbell

Margaret Hunter

Action = AssertTrust
User Name = 'mhunter'

As in the previous example, the administrator created an *XACML Access Control Domain* at the Deltawing entry. However, this time, they have also created:

- an *XACML Access Control Subdomain* at the Executive entry

The administrator has taken the same access policy shown in the previous example, and applied it to the XACML Access Control Subdomain.

Consequently, after starting the Authorization Policy Manager in trusted mode, Margaret Hunter would be able to manage policy within the subdomain.

As well as any restrictions declared by the access policy, there are inherent restrictions imposed by this type of delegation. The non-administrative user can create versions, policy and named expressions within the subdomain, but they cannot create attribute and role definitions. The only attribute and role definitions available to the non-administrative user are those inherited by the sub-domain.

XACML policy precedence

By default the rule in an XACML policy has a precedence of 0 (zero).

When the Policy Decision Point (PDP) receives an 'authorization decision request' it evaluates the rules with a precedence of 0. This gives a result of either 'permit', 'deny', 'indeterminate' or 'not applicable'.

When the result is 'not applicable', the PDP then evaluates rules with a precedence of 1. If this evaluation returns the same result, the PDP then moves onto rules with a precedence of 2, and so on. At any stage, if the result is anything but 'not applicable', the evaluation ends and PDP returns the result to the Policy Enforcement Point (PEP).

A rule's precedence can be set through either the ViewDS Management Agent or Authorization Policy Manager. It can be set to zero or any integer value (they do not need to be sequential) in order to override rules with a higher precedence value.

In summary, a rule with a precedence of zero overrides a policy with a precedence of 1, for example.

Authorization Policy Manager: Trusted mode

When the Authorization Policy Manager is in 'trusted mode', appropriate access is granted to a non-administrative user who has been delegated administration rights to XACML policy.

To start the application in trusted mode, enter either of the following from a command shell:

```
PAPui.jar -trusted
```

```
PAPui.jar -t
```

XACML role enablement

Role enablement is unavailable in this release of ViewDS, but will be available in a subsequent release.

In this release, areas of the ViewDS Management Agent and Authorization Policy Manager display role enablement as a greyed-out option.

VMA Settings window

The VMA's Settings window has been updated. Settings relating to the application log have been removed, and the following have been added:

- **Default connection timeout**
  Specifies the number of seconds after which the VMA will timeout when attempting to connect to a ViewDS server (RAS and DSA). Default: 3 seconds.
- **Automatically refresh connections**
  Specifies how frequently the Server View is updated. Default: 5 seconds.
- **Monitor connections for background reconnect**
  Indicates whether the VMA will periodically attempt to reconnect to any non-responsive ViewDS servers. This setting has no effect on a ViewDS server that you have intentionally disconnected through the VMA's Server View. Default: Selected.
- **Restore connections on startup**
  Indicates whether the VMA restores connections to ViewDS servers on start-up.

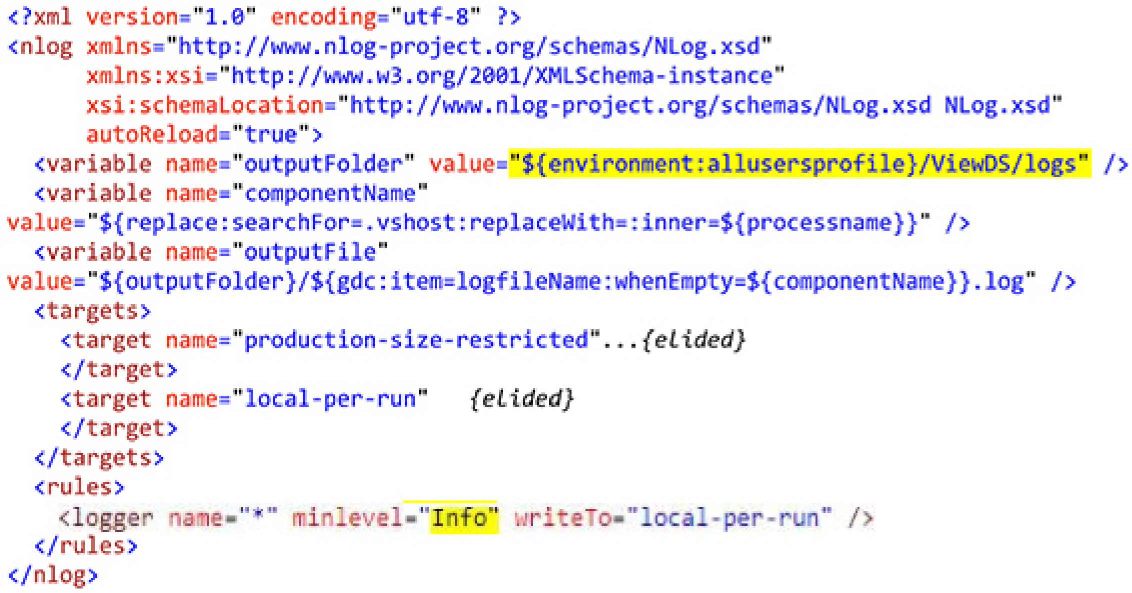
VMA error log

The ViewDS Management Agent (VMA) writes application errors to the VMA error log.

The functionality to view this error log has been removed from the VMA application. (The error log containing errors relating the DSA and associated components, however, is still available through the VMA.)

The VMA error log is now a text file and an implementation of the Nlog platform (see https://nlog-project.org/).

It can be configured through the `nlog.config` file located in the VMA installation folder. The configuration file allows you to specify the folder where the log will be written and the minimum logging level. The default settings are highlighted in the following example:



```
<?xml version="1.0" encoding="utf-8" ?>
<nlog xmlns="http://www.nlog-project.org/schemas/NLog.xsd"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="http://www.nlog-project.org/schemas/NLog.xsd NLog.xsd"
      autoReload="true">
  <variable name="outputFolder" value="${environment:allusersprofile}/ViewDS/logs" />
  <variable name="componentName"
value="${replace:searchFor=.vshost:replaceWith=:inner=${processname}}" />
  <variable name="outputFile"
value="${outputFolder}/${gdc:item=logfileName:whenEmpty=${componentName}}.log" />
  <targets>
    <target name="production-size-restricted"...{elided}
    </target>
    <target name="local-per-run"   {elided}
    </target>
  </targets>
  <rules>
    <logger name="*" minlevel="Info" writeTo="local-per-run" />
  </rules>
</nlog>
```

Where:

- `${environment:allusersprofile}` is synonymous with the `%ALLUSERSPROFILE%` environment variable, which is typically set to `c:\ProgramData`. Therefore, with the above configuration file, the VMA error log is written to `c:\ProgramData\ViewDS\logs`.
- `minlevel` specifies the minimum level of logging included in the VMA error log. For example, if the minimum level is Info, then Info, Warn, Error and Fatal are logged, but Debug and Trace are ignored.

The log levels, in descending order, are shown in the following table.

Level	Typical use
Fatal	Something bad happened; application is going down
Error	Something failed; application may or may not continue
Warn	Something unexpected; application will continue
Info	Normal behaviour like mail sent, user updated profile etc.

Level	Typical use
Debug	For debugging; executed query, user authenticated, session expired
Trace	For trace debugging; begin method X, end method X

There is one more level, Off. Since it is the highest value and is not used for entries, it disables logging when used as the minimum log level.

CORS support

ViewDS Access Sentinel now supports cross-origin resource sharing (CORS) policy.

The XACML Configuration tab in the ViewDS Management Agent (VMA) allows you to specify origins from which the Policy Decision Point (PDP) will accept requests.

All changes in ViewDS 7.5

COB-216

The 'emptyBag' function has been added to the 'Bag Functions' available in the XACML Expression window (ViewDS Management Agent and Authorization Policy Manager).

COB-747

`ODataDate` and `ODataTimeOfDay` have been added as available attribute syntaxes.

COB-899

See XACML policy precedence.

VIEWDS-690 and VIEWDS-691

See Import and export XACML policy.

VIEWDS-855

When a VMA user attempts to remove a supplier or consumer agreement, a confirmation box is now displayed.

VIEWDS-860

The new configuration-file parameter, `rastimeout`, defines how many seconds the RAS command line will wait for a response from the rassrv process before timing out.

The default value is 10; and a value of 0 declares an indefinite time limit.

You can override this setting from the RAS command line:

```
ras [-l seconds]
```

VIEWDS-1138

This release has been updated for OpenSSL 1.1.1b.

VIEWDS-1197

Previously, the only way to convert a shadow DSA to a master was to use a DAP modify operation that included the `manageDSAITPlaneRef` service control option. This can now be achieved through LDAP by using a new LDAP control that allows the DAP `manageDSAITPlaneRef` service control option to be provided as a control value.

VIEWDS-1200

For XACML access control, search-result processing in the DSA fetches the attributes of the subject for each entry that is checked. As the subject is the same in every case the attributes only need to be fetched once. Therefore, performance is improved and less memory is used by fetching the subject attributes only once per search.

VIEWDS-1256

The 'inRange' function has been added to the 'Date and Time Functions' available in the XACML Expression window (ViewDS Management Agent and Authorization Policy Manager). The 'inRange' function tests whether a specified time is within a given range while taking into account time zones.

VIEWDS-1262

Previous versions of ViewDS processed replication agreements one at a time, in series. While adequate, this was not scalable, and allowed single points of failure or latency to affect replication.

In this release, a supplier DSA processes replication agreements in parallel. Failure or latency associated with one replication agreement does not affect another. Additionally, a single supplier DSA can now handle a far greater number of consumers without lagging, which improves the propagation time.

VIEWDS-1274 and VIEWDS-1290

See Composition-time XACML delegation and Authorization Policy Manager: Trusted mode.

VIEWDS-1278

Passwords in `dsaCollaborators` values are encrypted in dumps, update logs and SDUA output. The whole `dsaCollaborators` value is encrypted in storage.

VIEWDS-1285

The DSA and Java PDPLiaison libraries have been updated to conform to the latest versions of the XACML REST and JSON profiles.

VIEWDS-1295

Improvements have been made to logging that relate to failed authentication.

VIEWDS-1297

See XACML role enablement.

VIEWDS-1300

See VMA Settings window.

VIEWDS-1311

See CORS support.

Bug fixes

COB-754

Fixed unnecessary chaining from shadow to master.

VIEWDS-637

When the RAS was installed as a Windows service (ras -i), a service entry was added without a description. The entry now includes a description.

VIEWDS-1067

With the demonstration directory, Deltawing, a DSA with a password policy implemented would stop unexpectedly after a user changed their password.

VIEWDS-1068

It was not possible to add the `viewDSPasswordQuality` attribute through the SDUA.

VIEWDS-1166

The Access Presence tags `<VFGCRequest>` and `<VFGCConfirm>` were generating a closing `</input>` tag, whereas HTML defines the tag as self-closing.

VIEWDS-1199

The ‘startsWith’ and ‘contains’ searches were taking a long time to process because there was no index support for the `literalStringSubstringsMatch` matching rule. Such searches resulted in a scan of all the eligible entries.

VIEWDS-1255

The following XACML time functions were not giving the correct results when time values included a time zone: time-equal, time-less-than, time-less-than-or-equal, time-greater-than, time-greater-than-or-equal and time-in-range.

`GeneralizedTime` values with fractional hours or minutes were not being compared correctly.

VIEWDS-1267

A VLV search for `(objectClass=*)` was returning real and administrative entries, including access control subentries.

VIEWDS-1276

An update operation that would succeed on the master DSA would fail if it were attempted on a shadow, from where the operation should have chained.

VIEWDS-1280

The DSA was dropping the connection to an Active Directory subordinate LDAP server if it received an unusually large LDAP message in a search result.

VIEWDS-1281

When dumping a database with the automatic indexing attribute set to ‘true’, no indexes beyond the predefined indexes were being built.

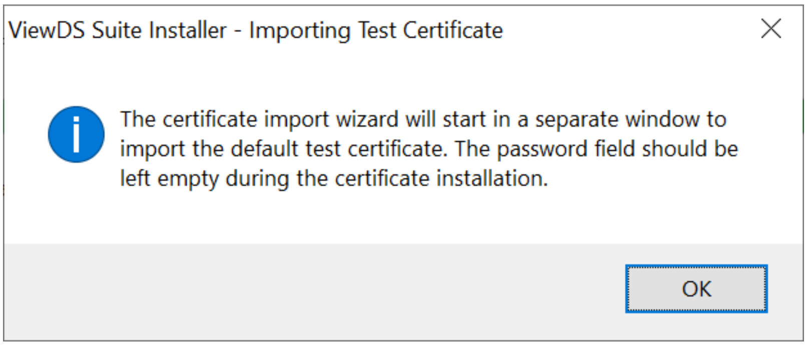
VIEWDS-1303

A spurious indexing error was being reported when attempting to remove XACML policy.

Known issues

The ViewDS VMA installer has one known issue.

During installation, a dialog is displayed to say that the Certificate Import Wizard will start in a separate window.



ViewDS Suite Installer - Importing Test Certificate

The certificate import wizard will start in a separate window to import the default test certificate. The password field should be left empty during the certificate installation.

After clicking **OK**, the installation process may appear to hang.

This is because the Certificate Import Wizard is hidden behind the ViewDS Suite installer.

After following the steps in the wizard, the installation process will continue.