



**Symantec Management Platform:
Agent Identity Management
High Level Design Document**

(PROJECT ORION)

Table of Contents

INTRODUCTION	3
DOCUMENT PURPOSE.....	3
OVERVIEW	3
ARCHITECTURE TEAM VISION/EAD	3
HIGH-LEVEL DESIGN	5
SEPARATE WEB SITE FOR NS AGENT	5
<i>Access from Gateway.....</i>	5
<i>Creation and configuration of secured Web Site</i>	6
<i>Securing the new web site</i>	8
NS Agent Identity	9
Web Services/Pages Configuration on Console Site.....	9
Web Services/Pages Configuration on Agent Site	9
Web Services available on secured site.....	10
<i>NS Upgrade</i>	10
<i>NS Agent Upgrade.....</i>	11
<i>Site Servers.....</i>	11
COMMUNICATION	12
<i>Certificate Management.....</i>	12
Agent Installation Package Creation	13
Package Registration	15
Permanent Certificate Requesting	16
Manual Certificate Request Validation.....	16
<i>Certificate Registration</i>	17
<i>Certificate Validation on Server</i>	18
<i>Certificate Validation on Client</i>	18
<i>Certificate Storage</i>	18
<i>Certificate Revocation.....</i>	18
<i>Certificates Remediation.....</i>	19
<i>Managed Client Redirection.....</i>	19
<i>Site Servers.....</i>	19
RESOURCE ACCESS LIMITATION	20
<i>Agent Identity Management.....</i>	20
NS Client Context Determination	21
“NS Agent Identity” Account Processing	22
<i>Resource Protection Next Phase</i>	22
REPORTS.....	23
<i>CEM Installation Packages Report</i>	23
<i>Certificate by Package Report.....</i>	23
<i>Certificate by Thumbprint Report</i>	24
<i>Related Certificates Report</i>	24
<i>Package Certificate Request Status Report.....</i>	25
<i>Certificate Request Queue Report.....</i>	25
APPENDIX A: ADDING CEM AND AGENT IDENTITY MANAGEMENT SUPPORT TO SOLUTIONS	26
APPENDIX B: DEFINING VIRTUAL APPLICATIONS FOR NEW AGENT SITE.....	27

Introduction

Document Purpose

The purpose of this document is to describe changes being made as part of the Orion release to implement the Agent Identify Management feature that is part of the Cloud-Enabled Management (CEM) functionality and to provide guidance regarding steps that solutions leveraging the Symantec Management Platform (SMP) may need to take as a result of these changes.

Overview

The Agent Identify Management feature will only be used by CEM agents in the Orion release. Non-CEM enabled NS Agents will continue to work in legacy mode and will not leverage the Agent Identify Management. This will allow backward compatibility of SMP for solutions and products which will not implement CEM support in the Orion release.

Architecture Team Vision/EAD

SMP introduces a new web site dedicated to managing clients using the CEM functionality. The web site is created during CEM functionality setup by the administrator and has a custom web root and a custom web application (and virtual directory) structure. By default, the web site will listen on custom port 4726. However, the administrator can customize the port number to be used.

All clients that are managed over the Internet will be automatically redirected by the SMP Internet Gateway machine to that web site. Clients on the internal network continue to use the SMP Console web site. The redirection happens automatically without any manual intervention.

Internal clients continue using the SMP Console web site, so that customers who do not need CEM functionality will not need to make any changes. This also eliminates the need to change other existing functionality, such as push install, pull install, site server communication, remote management functionality, etc.

The new web site for external Agents requires use of client certificates for authentication. It does not allow any other form of authentication. All solutions which provide web services to be consumed by the Agent over the Internet need to integrate with the dedicated external Agent web site. Services that are meant to be available only to computers on the internal network (for example, Deployment Solution) do not need to be made available on the dedicated web site.

In order to make it easier to provide proper client certificate checks inside solutions' web services, NS Core provides some helper functionality. This takes the form of configuring the certificate trust list for the web site and/or providing an HTTP handler to be injected into the ASP.NET pipeline by

editing Web.config. NS Core also provides helpers to find the identity of the client (e.g., its resource GUID), so that it could be used in subsequent security checks.

CreateResource.aspx and PostEvent.aspx that are provided through the Dedicated Agent Web Site have been changed so that they allow creating and reporting only specific resource types and resource associations. Specifically, the following entities are white listed:

- Resource types
 - Computer and its derivatives
- Software Resource Model (Software Product, Software Release, File, etc.)
- Resource Associations
 - Computer to Software Resource Model
 - Software Resource Model
- Data Classes
 - Related to Computer resource type and its derivatives
- Related to Software Resource Model

High-Level Design

Separate Web Site for NS Agent

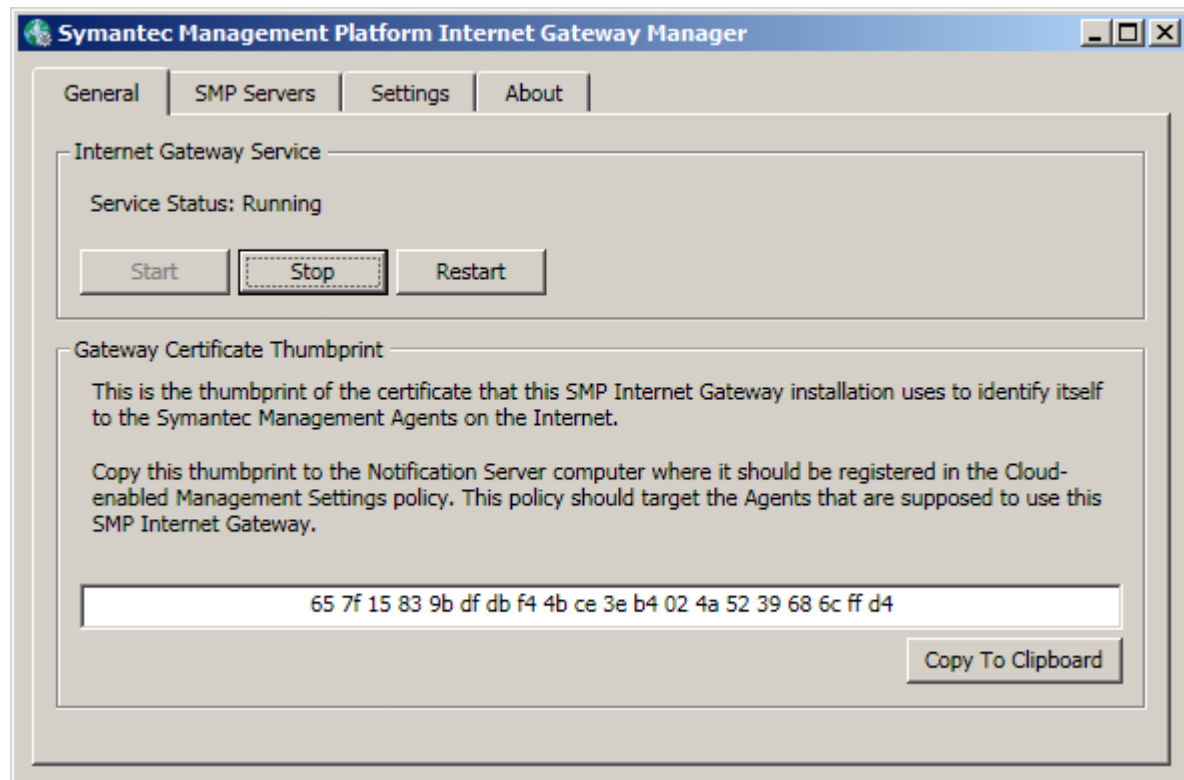
CEM-enabled NS Agents access this site over HTTPS and using only certificate authentication.. Non-CEM NS Agents (NS Agents from the local network) don't need, and will not be able to access, this site.

The legacy web site will be still used by SMP users, agents and agent plug-ins of the platform and its solutions in the Orion release. All agent-related pages and web services will stay on the old site and will be duplicated on the CEM site once it is configured.

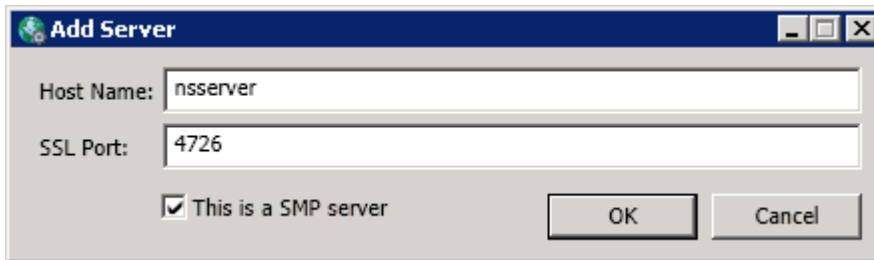
It is important to keep in mind that the redirection to the new site is transparent to the agent and all plug-ins and is done automatically by the SMP Internet Gateway. The NS Agent API will return the URL address to the old site only. All Symantec and third-party solution development teams must make modifications to their config files to use the new secured site if their plug-in requires it while working in CEM mode. If any plug-in has a logic that tries to establish a direct connection to the NS without using the Agent API, it will fail on CEM clients. In other words, it is the responsibility of plug-in developers to handle CEM use-cases.

Access from Gateway

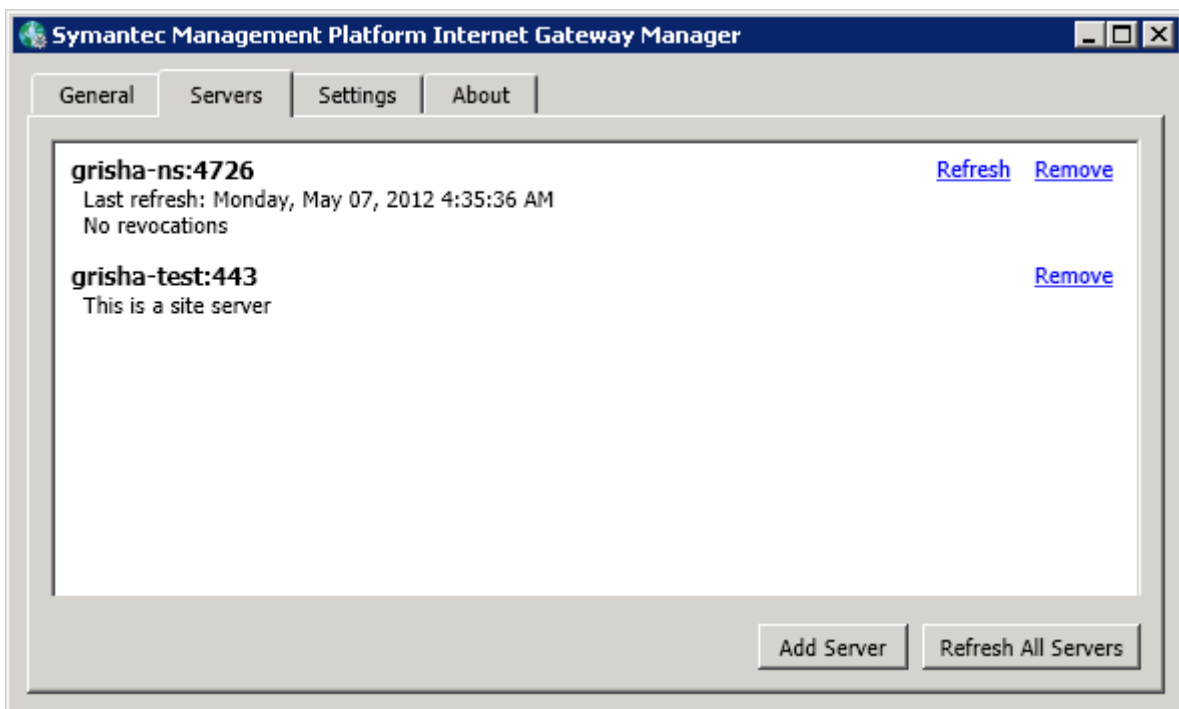
Symantec Gateway Manager, installed on the gateway, allows the configuring of CEM agent access to NS Servers.



While registering a NS Server, the administrator must specify an NS Server name and a CEM HTTPS port of the secured web site.



The gateway only allows access to the CEM HTTPS port of the secured site and routes all incoming calls from CEM NS Agents to it. This is done by filtering all incoming calls and substituting specified HTTPS port with the CEM port. So all calls go through the secured web site and certificate verification is applied on the server side.



Creation and configuration of secured Web Site

A new page is available in the SMP console, which allows configuration of the secured web site at any time after installation of the SMP. The user can configure HTTPS port used by CEM agents, as well as the web site name and certificate.

The page is located under 'Settings -> Notification Server -> Cloud-enabled Management' in the console menu and under 'Settings -> Notification Server -> Cloud-enabled Management Settings -> Agent Site Settings' in the All Settings tree. The page looks as follows:

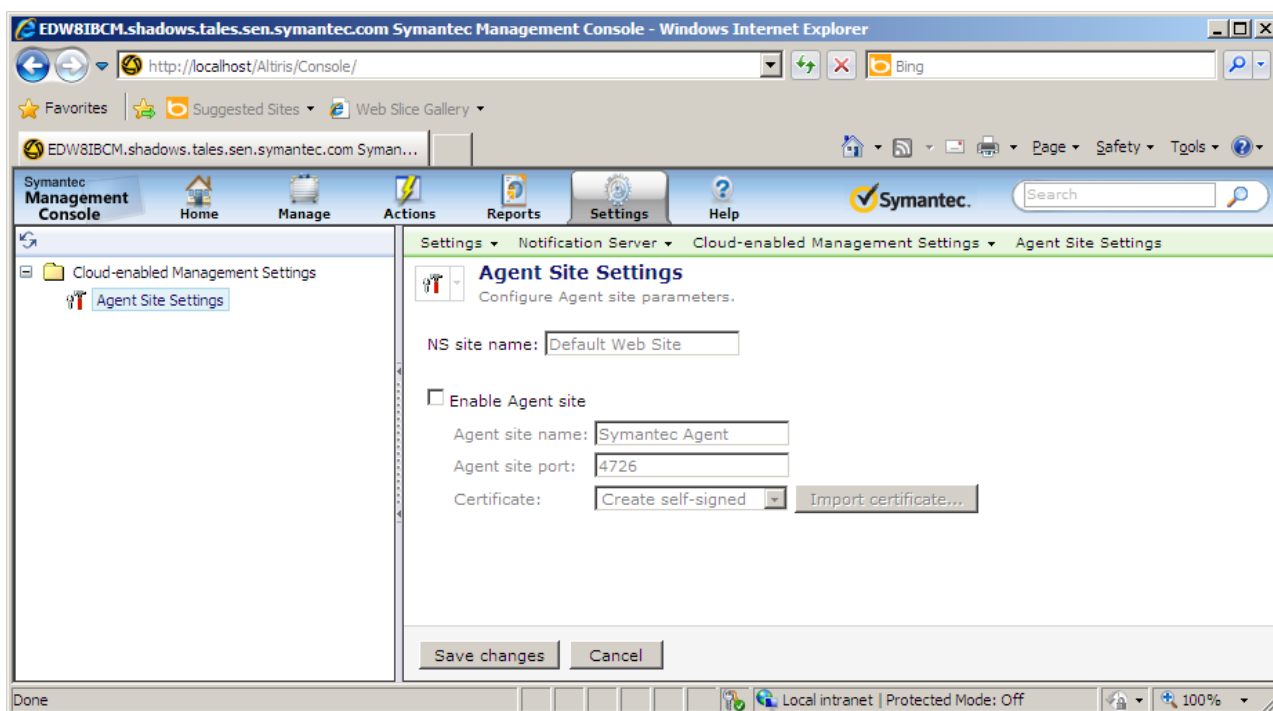


Figure 1. Agent Site Settings configuration page in Console

1. The 'NS site name' text box displays the name of IIS site where the SMP Console is installed. It is not editable by users.
2. The 'Enable Agent site' check box is unchecked by default and all controls below it are disabled as shown in Figure 1. When a user checks this checkbox, the controls below it will become enabled and editable.
3. The 'Agent site name' text box is used to specify the name of the new Agent Site. The site will be created automatically. When the 'Save changes' button is pressed, the value in the 'Agent site name' text box is validated to ensure that there is no site with the same name in IIS. If there is already a site with the same name in IIS, an error message is generated and shown on the top of the page.
4. The 'Agent site port' text box is used to specify the port of the new Agent Site, which is used for HTTPS binding. (The Agent Site will only support the HTTPS protocol. The Require SSL option will also be set to true.) When the 'Save changes' button is pressed, the value in the 'Agent site port' text box is validated to ensure that it is a positive number and that the port is not already in use in IIS.
5. The 'Certificate' combo box displays a list of available certificates on the machine located under the Personal folder. By default, a certificate is not specified and a self-signed certificate will be created.
6. Users can use the 'Import certificate' button to import their own certificate.

These settings are used to create and configure the secure web site, which looks as follows:

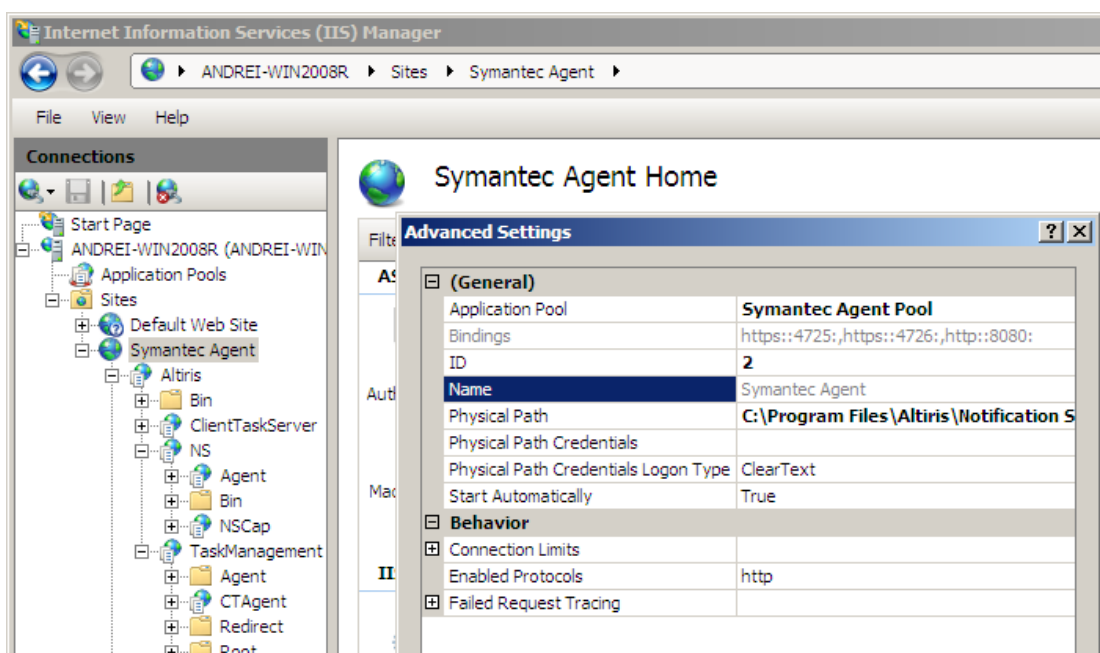


Figure 2. Configuration of secured web site in IIS

When the Agent Site is created, the 'Enable Agent site' check box becomes checked and disabled, and all other controls except 'Agent site port' also become disabled. The name and certificate cannot be changed after the Agent Site is created. However, the Agent Site port can be changed. Changing the value of 'Agent site port' text box and pressing 'Save changes' button updates the Agent Site port in IIS.

Each product that has something to publish for the Agent Site must have a configuration file which contains a list of virtual applications to publish (see Appendix B for more details). These configuration files are included in the product's main configuration file under a new <agentWeb> tag and are processed by a task executed on creation of the Agent Site. As a result, the described web applications are created under the new secured web site. On upgrade or reconfiguration of the Agent Site, the configuration files are processed to upgrade or restore the secured site. (It is also possible to specify in the configuration files that a virtual application should be removed, which might be required in upgrade scenarios). Once the site is created, it is not possible to disable it.

The site creation task enumerates all installed solutions, creates a list of configuration files and processes all <agentWeb> sections. After that, the manage distribution points portion of the task is executed for each active package and a PackageShare virtual application that contains the package codebases is created on the new Agent Site.

Securing the new web site

NS Agent Identity

A new internal account named 'NS Agent Identity' is created by the installation. This account does not have credentials assigned to it because it will be never impersonated and cannot not be used to log-in into the Console or the Agent site. However, this account does participate in the NS Resource Security Model and is used for setting the security context on the processing NS Events from Symantec Agents.

All required file system security permissions on the secured site are granted to the NS Agent identity automatically, during the installation and configuration of the secured site. All required NS permissions and privileges are granted to it during product installation (see [Agent Identity Management](#) section below).

Web Services/Pages Configuration on Console Site

The Console Site continues to have a full set of web pages designed for agent use. As before, they are defined in configuration files under the <webs> section:

```
<webs>
  <web name="ClientTaskServer" relativeDir="ServerWeb" anon="true" agent="true" />
</webs>
```

However, a new attribute `agent="true"` has been added. If this attribute is set to true, the virtual application will be created under the Symantec Agent AppPool. The Symantec Agent AppPool gets created by the NS Core configuration and is required for all web pages designed for the agent. All solutions must use this new attribute to separate their agent related virtual applications from their console related virtual applications.

Solutions that manually create agent related virtual applications can use the `Altiris.NS.Utilities.AgentSite.AgentSiteApplication.AddApplicationToAgentAppPool` method specifying the virtual path of their application (e.g. `"/Altiris/NS/Agent"`) as an input parameter.

Web Services/Pages Configuration on Agent Site

During the platform's installation, a new physical folder "C:\Program Files\Altiris\Notification Server\AgentWeb" (in case of default installation) is created. This folder contains a Root folder (which is a root folder for the new secured site) and an Agent folder (where an Agent virtual application is physically located).

During the product configuration, new virtual directories are created as specified in the configuration file components for publishing (web applications). Solutions should install their web pages designed for agent use as usual (in the same physical location), but additional IIS applications must be created under the new secured site according to the <agentWeb> section from the configuration files (which will point to the same physical location). If the Agent Site already exists, upgrade or reconfiguration will result in the processing of the <agentWeb> sections.

After creation of the Agent Site, the old Console Site and new Agent Site will have similar sets of virtual application used by the Symantec Agent.

Web Services available on secured site

The secured site exposes a limited set of web services that are required by the NS Agent and client side solutions to function properly. If a solution installs its own web services that are required by CEM clients, they must have a configuration file with their description as described above.

The platform installation places the following services under the secured web site:

- Altiris/NS/Agent – required by NS Agent.
- Altiris/NS/NSCap– required by NS Agent.
- Altiris/PackageShare – package server related service.

The structure of agent applications in the new secured web site is the same as it was previously in the old NS site and looks as follows:

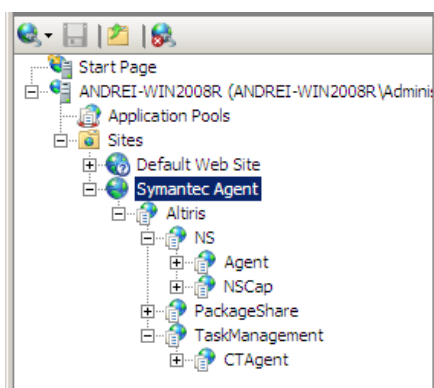


Figure 3. Structure of secured web site in IIS

NS Upgrade

On upgrade, a new secured site will not be created automatically (<agentWeb> nodes will not be processed). If the Agent Site was previously created (e.g. in the case of an on-box upgrade from SMP 7.5 and above) the <agentWeb> nodes will not be processed. If an IIS application already exists and upgrade mode is set to ignore in the configuration file, it will not be reconfigured. However, its content (web pages, etc.) can be changed if the MSI installs files to the same physical location. If the upgrade mode of the virtual application is set to overwrite in the configuration file then the application will be reconfigured. It is also possible to specify IIS applications that should be removed from the new secured site (for future upgrades). (See Appendix B for more details).

After being upgraded, the NS will have the same set of virtual applications on the Console Site. Thus, all agents will continue working with the Console Site.

This design assumes no changes in site server rollout. Preparation of site servers for a CEM client is the administrator's responsibility.

NS Agent Upgrade

Because the NS will have the same set of virtual applications on the Console Site after being upgraded and all agents will continue working with the Console Site as before, the agents will be upgraded as they previously were. (The agents will not be aware of the new site).

To change the port of the secured site (e.g. to use a non-standard port as part of a security hardening procedure), administrators should use the Agent Site Settings page in the Console (see Figure 1). Manual reconfiguration of IIS is not supported. After changing the port on the Agent Site Settings page, administrators should go to the Gateway and specify the new redirection port for the NS. This port change procedure will not impact the Symantec agents, as it only affects the Gateway.

Site Servers

To expose some of their site servers for the CEM Agents (servers that are behind the gateway), an administrator must configure them manually by switching to HTTPS and installing certificates that are required to perform validate incoming connections from NS Agents.

Site servers that are located outside the NS local network work as is and must not be configured for Agent Trust.

Communication

Within an established tunnel to an SMP Internet Gateway, an NS Agent establishes an SSL connection to the CEM web site. Only certificate authorization schema is supported. While SSL communication is already an implemented option, certificate authorization is added as a part of the Agent Identity Management feature. X.509 format is used for certificates. Certificates are issued by the NS Server and NS command line tools and registered in the NS database associated with particular clients. On web interfaces call, certificate information are extracted from HTTP request context and used to validate the caller (i.e., check that the certificate that was used during authentication is registered). An SMP Server API provides a class that deals with certificates validation on the SMP Server; site servers perform validation on their own.

The following diagram shows certificate usage of CEM agents working with NS and gateway.

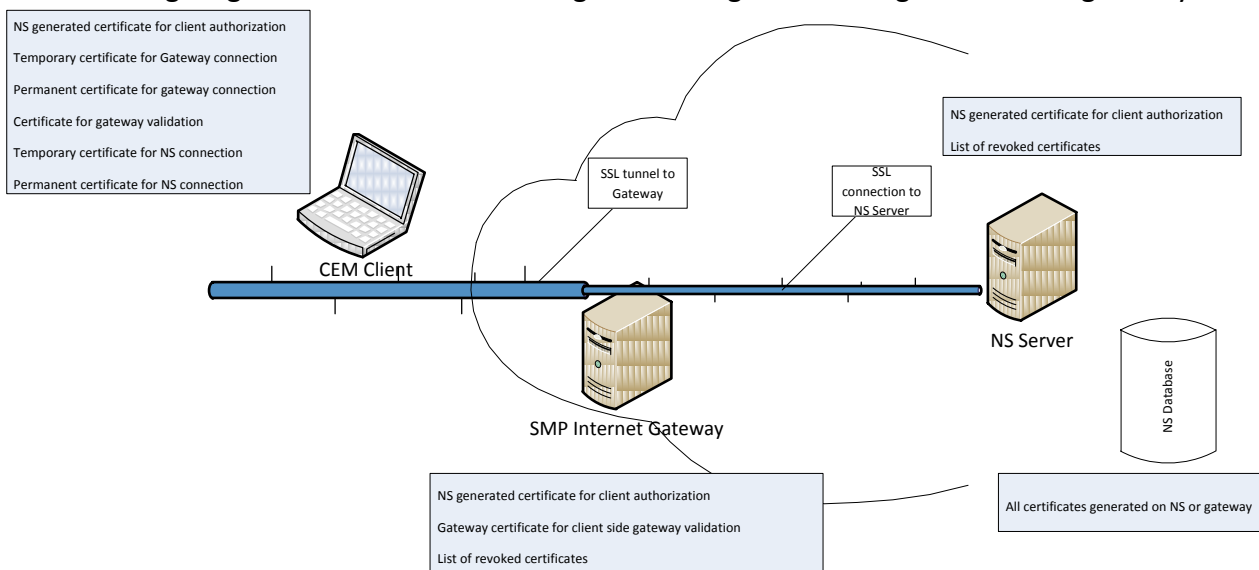


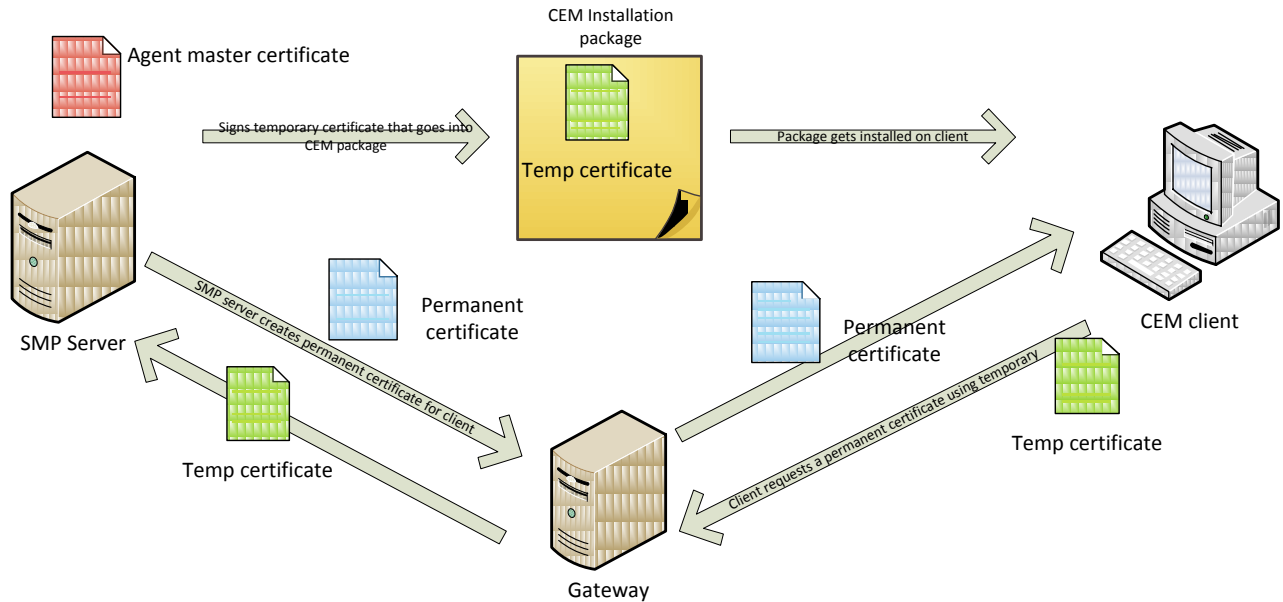
Figure 4. Diagram of certificate usage of CEM agents working with NS and gateway

Certificate Management

As stated in the overview, the Agent Identity Management feature in the Orion release will be used by CEM agents only. The CEM agent installation package contains (along with certificates required to access the gateway) a temporary certificate issued during package creation that is used to connect to the NS Server. As soon as a connection is established, the agent requests a permanent certificate from NS; this one is used in subsequent calls. No other calls can be performed using the temporary certificate. By default, the temporary certificate is valid for 7 days. If during the package is not installed or the client was not able to connect to the SMP Internet gateway during this period, the certificate expires and another package must be created/delivered.

In order to allow certificate authorization, an NS Agent master certificate must be installed on the client and the gateway. On the gateway, it is obtained when NS is added to the list of allowed

servers. On clients, it is present in the CEM offline installation package and delivered with the CEM policy. The Package also contains a thumbprint of the Gateway certificate that is used by the NS Agent to ensure that the NS server to which it connects is the correct one.



Agent Installation Package Creation

While configuring the CEM agent installation package, the current dialog

Symantec Management Console

Cloud-enabled Agent Installation Package

Operating System:

Policy (Internet Gateways):

Organizational Group:

Installation Name:

Expiry: Date: Time: :

☒ Automate certificate distribution

☐ Limit number of issued certificates to:

IP mask:

☐ Sign using

File:

Password:

Thumbprint:

☐ Encrypt package

This installation name is shown on the subject line of the Agent certificate attached to the installer, and can be used for reporting and diagnostic purposes. For a single computer installation, you may want to use the name of the computer or the primary account. For a package that will be installed on multiple computers, you may want to use the appropriate office or department identifier.

Warning:
The Cloud-enabled Agent installation package is valid for a limited period of time. By default, it is valid for seven days from the time that it was generated. If you use this package to install the Agent after it has expired, the installed Agent is not able to use the SMP Internet gateway for communication. You then have to reinstall the Agent using a newly generated installation package.

is extended with several controls related to permanent certificate distribution schema:

- **Expected number of permanent certificates:** The administrator can specify an expected maximum number of clients that will be installed using this package. It is not possible to obtain more permanent certificates from the server using the temporary certificate included in this package. This prevents certificates spoofing in case of a stolen CEM offline Installation package.
- **Automatic certificate distribution option check box:** The administrator can automate permanent certificate distribution by enabling it. In this case the SMP server issues a permanent certificate to the caller automatically, skipping manual certificate validation. If the administrator is sure that the package distribution channel is safe, the administrator can avoid manual certificate validation steps. Otherwise, the administrator will be responsible for certificate requests approval (Manual Certificate Request Validation).
- **Client IP mask:** Optional IP address mask that, if specified, is used during permanent certificate issuance to validate the caller. If the administrator knows exactly the IP address pattern of agents that will install the CEM package, the administrator can specify it and the NS server will reject certificate requests from IPs that do not pass the mask check.

- Encrypt package: by checking this check box and specifying an encryption password, the administrator can secure package content. The created package is encrypted, and the end user is required to provide a password to access package content (perform package installation).

These settings are available in the SMP database for a successfully created package.

Package Signing

To ensure that a package comes from a trusted source and was not modified on its way, a “Sign using” option to digitally sign package is available in the package creation dialog. The administrator is able to specify a certificate to be used to sign the created package. It must be any code signing compatible certificate that contains a private key. The certificate source can be either a local certificate storage (thumbprint of a certificate must be specified in this case) or a “pfx” certificate file. The administrator can sign a package with a certificate that is trusted by an organization where the package will be delivered.

A package also can be signed manually by third party tools like MS SignTool.

Package Registration

All successfully created packages get registered in the SMP database. Corresponding reports allow the administrator to review created packages and list certificates (temporary and permanent) associated with the package.

A database table contains following information:

- Package ID
- Package OS type
- ID of associated policy
- Organizational group ID
- Package description
- Package expiration time
- XML with certificate distribution settings

All generated certificates are linked to a package by package ID (described in section “Certificate Registration”).

Permanent Certificate Requesting

An NS Agent performs a permanent certificate request on start, as a first action. Depending on the certificate validation type selected during package creation:

- **Automatic Validation:** The SMP server generates a permanent certificate and returns it to the client. This option is selected by default.
- **Manual Validation:** The SMP Server places a certificate generation request in queue (in a dedicated table, the request contains several client details – IP, request time, link to temporary certificate used in request, company name, etc.) and returns “request pending” status to the NS Agent. The administrator is responsible for verifying pending certificate requests in the NS console to validate or decline them. The NS Agent will keep polling the server for a certificate. As soon as the request gets validated, the NS agent receives a generated permanent certificate.

The SMP server count certificates issued for a particular package (certificates requested using a temporary certificate from a package). When the “issued” counter reaches the maximum number of certificates specified during package creation, the server declines certificate generation requests from clients that are using an associated temporary certificate.

Manual Certificate Request Validation

In a case where an administrator is unsure about package distribution channel security and suspects that a package can be lost or stolen, a manual certificate validation option can be specified during package creation. When this option is used, SMP Agents do not obtain permanent certificates directly; rather, they submit certificate requests providing client details (name, company name, etc). Requests get registered in a dedicated table in the SMP database, waiting for administrator approval. The administrator can review these requests in the SMP Console and allow or decline them. If the request is approved, an SMP Agent receives a generated permanent certificate on the next polling call. The approved request remains in queue until the parent temporary certificate expiration time. On schedule (daily hidden server policy) the queue is checked by the server and cleaned of expired requests. If a temporary certificate expires before a permanent certificate was received, the agent will not be able to connect to the SMP Server and the approved request will be removed from the queue on the next schedule activation.

Certificate Registration

All certificates issued by NS Server or NS certificate processing tools are registered in the NS database in a table that was introduced with CEM related changes (the table has been extended to contain more fields that are used in reports).

```
CREATE TABLE [dbo].[CertificateRegistration]
(
    [Guid] [uniqueidentifier] NOT NULL,
    [ResourceGuid] [uniqueidentifier],
    [ParentGuid] [uniqueidentifier] NOT NULL,
    [Scope] [nvarchar](220) NOT NULL,
    [ThumbPrint] [nvarchar](100) NOT NULL,
    [SerialNumber] [nvarchar] (100) NOT NULL,
    [ExpirationDate] [datetime],
    [SubjectDN] [nvarchar] (max) NOT NULL,
    [Issuer] [nvarchar] (100) NOT NULL,
    [Certificate] [varbinary] (max) NOT NULL,
    [CertificateState] [int] NOT NULL,
    CONSTRAINT [PK_CertificateRegistration] PRIMARY KEY CLUSTERED
    (
        [ID] ASC,
        [Scope] ASC
    )
) ON [PRIMARY]
```

- **Guid** – internal certificate identification,
- **ResourceGuid** - for permanent client certificates, contains client computer resource ID (*resourceid_guid*). This is a 1:1 relation, so it means that a certificate identifies a computer it is issued for.
- **ParentGuid**- specifies a policy or package that an ID certificate was issued for.
- **Scope** – certificate purpose and scope (gateway certificate, client temporary certificate, client permanent certificate etc). Possible values: “R” and “O”, “Site Certificate” (used during CEM agent registration to associate NS Agent resource ID with an organizational group or resource target.)
- **Thumbprint** – certificate thumbprint.
- **SerialNumber** – certificate serial number.
- **ExpirationDate** – certificate expiration date (NULL if it is permanent certificate).
- **SubjectDN** – certificate subject.
- **Issuer** – issuer.
- **Certificate** – certificate itself.
- **CertificateState** – certificate status flags: 0 – normal, 1 – revoked.

This table is used by reports allowing the administrator to locate certificate details for a particular managed computer. Additional indexes will be added as required.

Certificate Validation on Server

A certificate is assumed to be valid if it passes IIS authorization during connection and is registered in the SMP database.

Since a secured web site will be configured only for HTTPS access, IIS will decline connections performed without certificates. In order to protect traffic from CEM agents, the NS server performs additional verification of connections coming in on the HTTPS port that is exposed to the gateway. If a call is performed on this port, the NS Server checks that it is signed with a certificate and that this certificate is known as an Agent Trust permanent certificate.

Temporary certificates have restricted rights on the SMP Server. With a temporary certificate it is only possible to request a permanent certificate; other calls will be blocked.

In the same way as CEM certificates are designed and implemented, issued NS certificates are controlled using CRLs.

Certificate Validation on Client

Clients use an IIS certificate (without private key) to validate the NS Server to which they connect.

Site Servers for CEM clients use their own certificates issued from the NS server. These certificates are signed using an NS master certificate which ensures that all clients are able to validate them. The site server certificates must be deployed to site servers for CEM clients manually by the administrator.

Certificate Storage

On the NS Server, issued certificates are stored in the NS Database in encrypted form. On the NS Agent side, certificates are stored in the certificate storage under Service\Personal.

Certificate Revocation

If a particular computer is compromised (hacked, lost, stolen) the administrator can revoke access to the NS server for this computer. In the case of a permanent certificate, the administrator can open an NS console and locate details about the compromised certificate for this computer (associated with certificate NS Agent resource ID, thumbprint or serial number). A temporary certificate that is located in an offline installation package is not associated with a particular computer but can be found by association with CEM installation packages (there are corresponding reports available). The Console provides an ability to revoke a certificate from certificate reports via the right-click menu. After a certificate is revoked, NS starts blocking incoming calls from the compromised computer.

Revocation of gateway and site server certificates has to be done manually. A CRL list will be propagated to site servers manually by the administrator. On the gateway CRL list import is configured based on schedule. Periodically the gateway pools NS Server downloading CLRs.

It is also possible that compromised certificate details can be obtained from the SMP Internet Gateway log. A command line tool (AexRevokeCertificate.exe) can be executed by the administrator on SMP to revoke the compromised certificate.

NOTE: A new report (see below in the document) has been created that allows the administrator to obtain certificate details required for certificate revocation.

Certificates Remediation

After compromised certificate revocation (compromised computer was hacked), NS agent calls from that computer are blocked. To resolve this situation the administrator has the following options:

1. **Agent reinstallation:** The administrator can re-create a CEM installation package that contains new temporary certificates and delivers it to the compromised computer. CEM NS Agent will be re-installed; a new permanent certificate will be obtained by the Agent and registered for this computer.
2. **Certificate reset with temporary certificate:** The administrator can create a temporary certificate using a command line utility (AexGenerateClientCertificate.exe) and deliver it to the compromised computer. The certificate must be manually placed in the client certificate store and NS agent registry will be populated with this certificate thumbprint; then it will be used to access the NS Server to get permanent certificate.

Managed Client Redirection

Redirection of CEM client from one NS to another can be performed only through the NS agent reinstallation process. The administrator can generate a CEM installation package on a second NS and perform client reinstallation. There is no automation for this process (for non-CEM clients it can be done via policy). ***NS agent with an enabled CEM policy ignores the part of the configuration policy that is related to NS switching.***

Site Servers

Site servers that support CEM agents must take into consideration:

1. Access to the site server must be configured on the gateway. This must be done manually by the administrator.
2. The site server web site must be configured on HTTPS with certificate authorization. This is a manual configuration of an already existing site server.
3. **The Certificate chain that is required to perform client certificate validation on the site server** must be obtained from the NS Server. This will be done by manual certificate installation, in the same way as it is expected to be done on a CEM client.
4. In the case of a compromised certificate, certificate revocation must be performed on a Site Server manually. A certificate revocation utility can create a revoked certificates list that the administrator will deliver on the site server and add to CRL.

Resource Access Limitation

This Agent Identity Management initiative addresses issues inherent in the processing of Notification Server Events (NSE's) sent by CEM Agents (i.e., Agents installed on computers outside the internal network) to the NS. Since processing of NSE's results in additions to, modifications of and deletions from the NS database, the NSE processing mechanism for data sent by CEM Agents needs to protect against compromised CEM Agents.

Agent Identity Management

In order to raise the level of data protection, Agent Identity Management introduces a role-based security schema that limits access to NS resources from Symantec Agents. Solutions that are claimed to be compatible with the Agent Identify Management standards in this document must review their resource manipulation schema since access to resources from an NS Agent will be restricted by the NS Server.

A new account resource NS Agent Identity is defined in NS configuration files, which is created during the configuration process. It appears in the NS Console under Account Management.

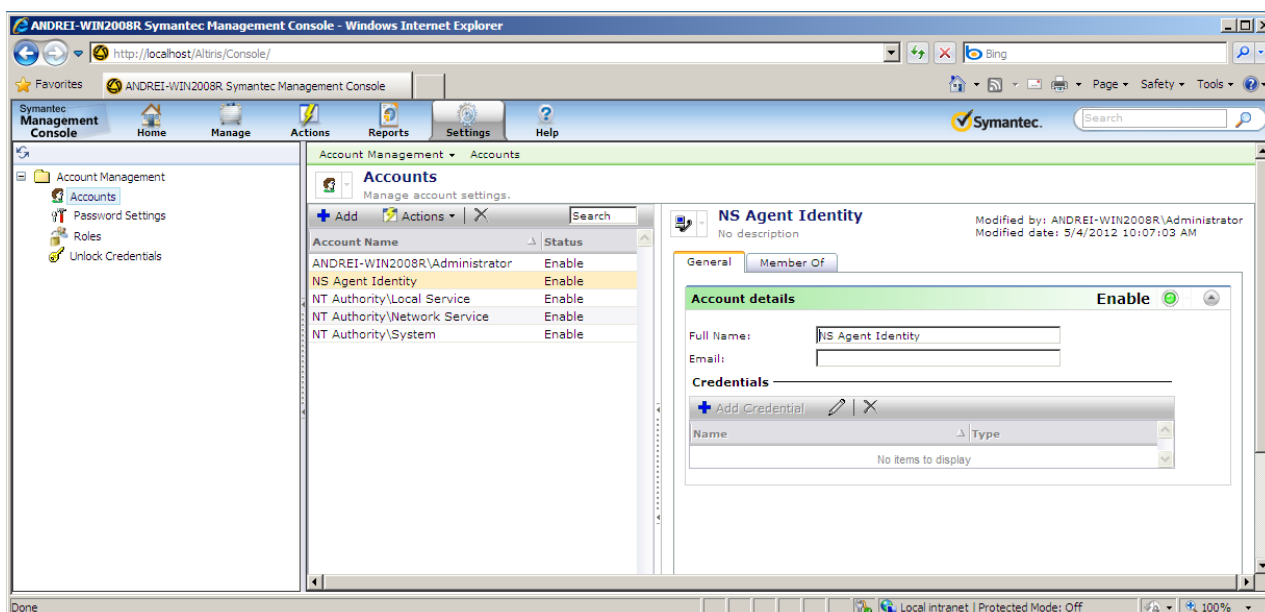


Figure 5. NS Agent Identity account in Console

As there is only one NS Agent Identity account with a constant GUID, there is no need to create a special role for it. All NS permissions and privileges are granted directly to the NS Agent Identity trustee (using the standard mechanism through configuration files, which are not new for solutions that will be responsible for granting access to this account to any items/resources that their plug-in may access). Although this account will not be hidden, any attempt to add it to any role in the UI or assign any credentials to it will be denied.

NS Client Context Determination

On an incoming request, a web service checks for the type of authorization that was used and, in the case of certificate authorization, extracts certificate details from the request. Using certificate details, a certificate type will be validated. If a certificate is registered in the NS database and is not a temporary one (under a temporary certificate only a permanent certificate request and initial computer registration are possible), the message is processed further.

With the resource creation web interface ([CreateResource.aspx](#)), the message is processed within the web call, so no special handling is required. This is not the case, however, with NSE processing – messages are placed in a queue and processed later by an NS Service.

In the case of NSE processing, an NSE will be placed in a queue (as it is in previous NS versions) along with metadata specifying that it is a NSE issued from an NS Agent.

A new table has been added to the NSE database: *EventQueueEntryMetaData*.

```
CREATE TABLE [dbo].[EventQueueEntryMetaData]
(
    [Id] bigint PRIMARY KEY IDENTITY NOT NULL,
```

```

        [EventEntryId]    bigint NOT NULL,
        [MetaDataTypeId] int NOT NULL,
        [MetaData]        nvarchar(3000) NOT NULL,
    )

```

- **ID** – metadata entry identification (key).
- **EventEntryId** – event entry identification -- ID from `EventQueueEntry` table to link queued entry with its additional data.
- **MetaDataTypeId** – identifies metadata content type. 0 means “Guid”; other values will be defined as soon as required.
- **MetaData** – metadata -- some XML that contains additional data describing the queued NSE.

For NSEs passed from NS Agents, an entry specifying that this entry belongs to an NS Agent is added to this table. *MetaData* specifies certificate details.

“NS Agent Identity” Account Processing

During NSE extraction from a queue, such metadata is extracted and, if it exists, the NSE processing thread sets the security context of NS Agent Identity using [SecurityContextManager](#), that forces the call to be performed from the name of NS Agent Identity.

With the resource creation web interface ([CreateResource.aspx](#)), security context is set to the caller (NS Agent Identity) and then the call is impersonated under NS Identity to allow the NS API to work.

Resource Protection Next Phase

The described resource access limitation is not a comprehensive security solution in and of itself, since the scope of accessible resources remains relatively broad. To complement this approach, each solution must have a role that lists access to required resources. Also, the solution’s resource model must be changed to define a resource owner – a computer that owns particular resources. Using certificates, NS Server will define an owner (a certificate identifies a resource ID it is associated with) and access is allowed only to resources that belong to caller.

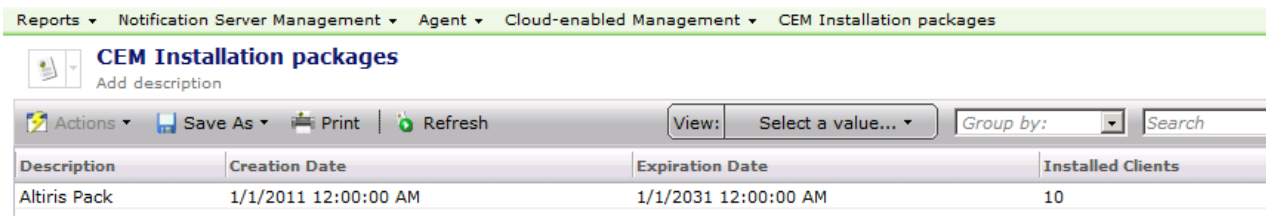
Reports

CEM Installation Packages Report

This report lists CEM offline installation packages created from the NS Console. The following columns are shown:

- **Package description:** package description specified by the administrator during package creation.
- **Creation time:** time when the package was created.
- **Expiration time:** embedded in package temporary certificate expiration time; after this time installations with this package will not be possible.
- **Installed Clients:** the number of CEM agents installed with this package.

By double clicking on a selected row, the administrator is presented with “**Certificate by Package Report**”.



Description	Creation Date	Expiration Date	Installed Clients
Altiris Pack	1/1/2011 12:00:00 AM	1/1/2031 12:00:00 AM	10

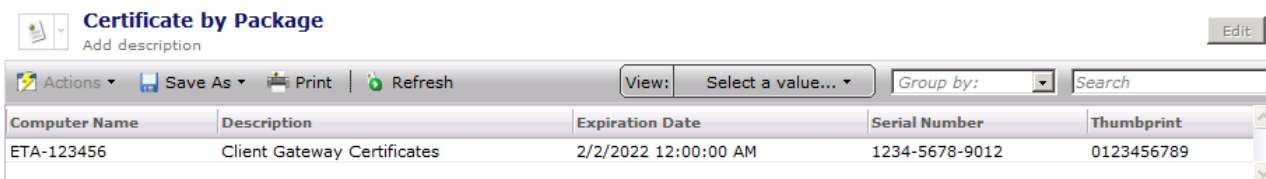
Certificate by Package Report

This report shows all certificates associated with a selected package (temporary and permanent). The following columns are shown:

- **Computer name:** name of computer that uses issued the permanent certificate.
- **Description:** certificate description.
- **Certificate expiration time.**
- **Certificate Serial Number.**
- **Certificate Thumbprint.**

By double clicking on a selected row, the administrator is presented with Resource Manager, showing information about the agent where the certificate is used.

The right-click menu includes an option to revoke selected certificate(s).



Computer Name	Description	Expiration Date	Serial Number	Thumbprint
ETA-123456	Client Gateway Certificates	2/2/2022 12:00:00 AM	1234-5678-9012	0123456789

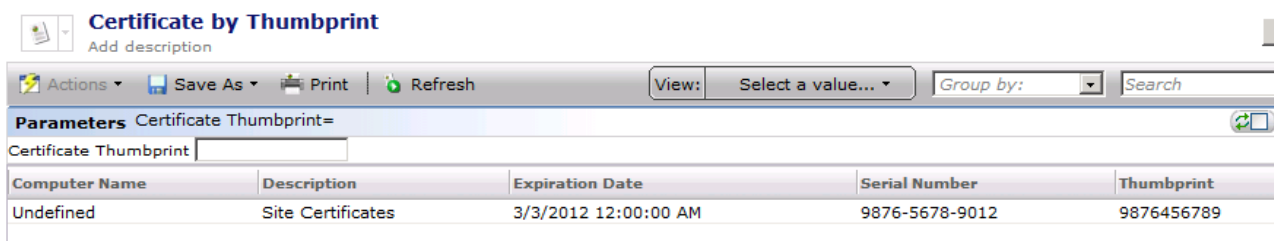
Certificate by Thumbprint Report

This report shows a certificate found by a certificate thumbprint specified as a parameter. The following columns are shown:

- **Computer name:** name of the computer that uses the issued permanent certificate ("Undefined" for temporary certificates).
- **Description:** certificate description.
- **Certificate expiration time.**
- **Certificate Serial Number.**
- **Certificate Thumbprint.**

By double clicking on a selected row, the administrator is presented with Resource Manager, showing information about the agent where the certificate is used.

The right-click menu includes an option to revoke selected certificate(s) or locate certificates related to the selected one via "**Related Certificates Report**".



Computer Name	Description	Expiration Date	Serial Number	Thumbprint
Undefined	Site Certificates	3/3/2012 12:00:00 AM	9876-5678-9012	9876456789

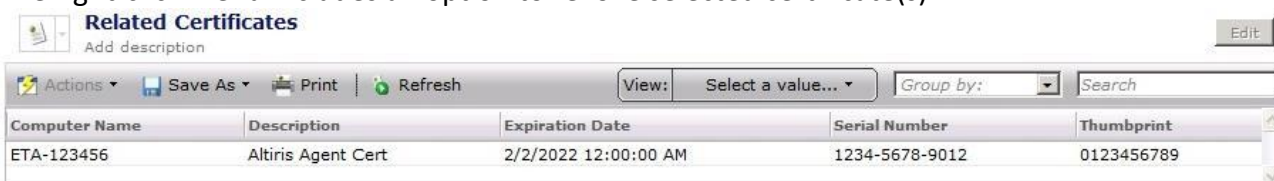
Related Certificates Report

This report shows a certificate related to a specified certificate. For a permanent certificate it will be a temporary certificate that was used to obtain it. For a temporary certificate it will contain a list of permanent certificates that were issued with it. The following columns are shown:

- **Computer name:** name of the computer that uses the issued permanent certificate.
- **Description:** certificate description.
- **Certificate expiration time.**
- **Certificate Serial Number.**
- **Certificate Thumbprint.**

By double clicking on a selected row, the administrator is presented with Resource Manager, showing information about the agent where the certificate is used.

The right-click menu includes an option to revoke selected certificate(s).



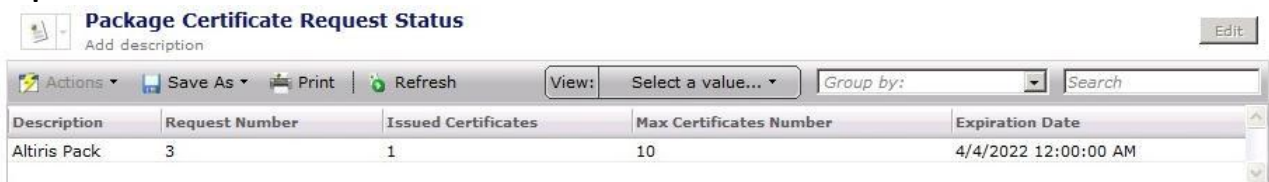
Computer Name	Description	Expiration Date	Serial Number	Thumbprint
ETA-123456	Altiris Agent Cert	2/2/2022 12:00:00 AM	1234-5678-9012	0123456789

Package Certificate Request Status Report

This report shows a list of CEM offline installation packages that have pending certificate requests available. The following columns are shown:

- **Package description:** package description specified by the administrator during package creation.
- **Requests number:** number of pending requests.
- **Number of issued certificates:** number of certificates already issued for this package.
- **Max number of certificates:** maximum number of certificates that can be issued for this package.
- **Expiration time:** embedded in package temporary certificate expiration time; after this time installations with this package will not be possible.

By double clicking on a selected row, the administrator is moved to ‘**Certificate Request Queue Report**’.



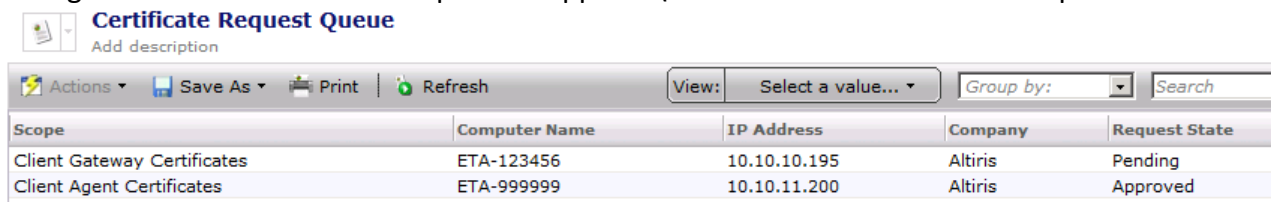
Description	Request Number	Issued Certificates	Max Certificates Number	Expiration Date
Altiris Pack	3	1	10	4/4/2022 12:00:00 AM

Certificate Request Queue Report

This report shows a list of certificate requests for a selected package. The following columns are shown:

- **Scope:** requested certificate scope (certificate to be used to connect to gateway or NS server).
- **Computer name:** name of the computer the request was performed from.
- **Company name:** name of the request submitter’s company.
- **IP Address:** IP of computer the request was performed from.
- **Request state:** request status: pending\approved\declined.

The right-click menu includes an option to approve\decline selected certificate requests.



Scope	Computer Name	IP Address	Company	Request State
Client Gateway Certificates	ETA-123456	10.10.10.195	Altiris	Pending
Client Agent Certificates	ETA-999999	10.10.11.200	Altiris	Approved

Appendix A: Adding CEM and Agent Identity Management support to solutions

- **Web Site Configuration:** Solutions need to split user-facing or integration pages and web services from agent facing web services. Agent-facing web services must be duplicated in the secured web site (since it will have a separate port and certificate authentication is configured on a web site, not web folder level). Console-facing web services must stay in the legacy web site only.
- **Dedicated Web Sites:** If a solution can install its own web site, it must be configured to use HTTPS and certificate authorization schema only. It is up to each solution how that will be performed.
- **NS Access:** Solutions must perform access to the NS server from the agent side using only NS Agent API. No direct connections (i.e., connections not through the NS Agent) to NS web sites will be possible. This will be a breaking change for some solutions.
- **Resources registration:** To allow NS Server to perform solution resources processing, solutions must register resources that can be accessed as a result of a call from an agent under the “NS Clients” role.
- **Site Server:** No changes on site server side are expected. Configuration of site servers for CEM clients will be manual in the Orion release.

Appendix B: Defining Virtual Applications for new Agent Site

The format for defining virtual applications for a new Agent Site in the configuration files is as follows:

```
<agentWeb>
  <application installMode="add" upgradeMode="ignore" virtualPath="/Altiris"
physicalPath="\Notification Server\AgentWeb" allowBrowseBinDirectory="true"
sharable="true" authentication="a" />
</agentWeb>
```

`<agentWeb>` node can contain as many `application` nodes as required. `application` node has the following attributes:

1. `installMode` (Optional), which has four possible values:
 - a. `Add` - adds specified virtual application to Agent Site (Agent Site pool will be used as Application Pool);
 - b. `AddConsole` - adds specified virtual application to Console Site;
 - c. `Remove` - removes specified virtual application from Agent Site;
 - d. `RemoveConsole` - removes specified virtual application from Console Site;
 - e. Default value - if `installMode` attribute is missing or its value is unknown, then `Add` mode will be used by default.
2. `upgradeMode` (Optional), which has two values:
 - a. `Overwrite` - overwrites specified application on adding if it already exists;
 - b. `Ignore` - skips adding specified application if it already exists;
 - c. Default value - if `upgradeMode` attribute is missing or its value is unknown, then `Ignore` mode will be used by default.
3. `virtualPath` (Mandatory), which specifies IIS virtual path of application starting from site root.
4. `physicalPath` (Mandatory for `Add` and `AddConsole` `installMode` and should exist on machine; Optional for `Remove` and `RemoveConsole` `installMode`), which specifies physical path of application starting from Altiris root (by default - "C:\Program Files\Altiris").
5. `allowBrowseBinDirectory` (Optional), which specifies whether this application needs to browse the `bin` directory, which is denied in IIS by default (most probably this option will not be used by solutions). If the `allowBrowseBinDirectory` attribute is missing or its value is not equal to `true`, then `false` will be used by default.
6. `sharable` (Optional), which specifies whether this application is able to share files like `/Altiris/PackageShare` or `/Altiris/NSCap/Bin`, for example (it makes the specified virtual application browsable and makes other changes required for share configuration). If the `sharable` attribute is missing or its value is not equal to `true`, then `false` will be used by default.
7. `authentication` (Optional), which specifies authentication of virtual application, allowed values are:
 - a. "a" - anonymous
 - b. "b" - basic
 - c. "d" - digest

- d. "w" - windows
- e. all combinations of the letters above, for example, "aw" - anonymous and windows authentications will be enabled.

All attribute values are not case-sensitive.

Common usage could be as follows:

- Adding virtual application to Agent Site:
`<application installMode="add" upgradeMode="ignore" virtualPath="/Altiris" physicalPath="\Notification Server\AgentWeb" />`
- Removing virtual application from Console Site:
`<application installMode="RemoveConsole" virtualPath="/Altiris" />`