

Installing, Configuring, and Troubleshooting the Online Responder (Microsoft's OCSP Responder)

Microsoft Corporation

Published: February 2008

Avi Ben-Menahem, Lead Program Manager, Microsoft Corporation

Editor: Debbie Swanson

Contributors:

Vishal Agarwal, Development Lead, Microsoft Corporation

Saurav Sinha, Developer, Microsoft Corporation

Oded Shekel, Program Manager, Microsoft Corporation

Jen Field, Program Manager, Microsoft Corporation

Shawn Corey, Software Development in Test, Microsoft Corporation

Rashmi Jha, Software Development in Test, Microsoft Corporation

Darren Bennett, Software Development in Test, Microsoft Corporation

Kelvin Yiu, Senior Program Manager, Microsoft Corporation

Yogesh Mehta, Program Manager, Microsoft Corporation

Abstract

This white paper describes the concepts behind and steps needed to install, configure, and troubleshoot the Online Responder, which is Microsoft's Online Certificate Status Protocol (OCSP) responder. The Online Responder is a role service that is used to implement OCSP revocation checking in Active Directory Certificate Services (AD CS) environments.



Copyright Information

This document supports a preliminary release of a software product that may be changed substantially prior to final commercial release, and is the confidential and proprietary information of Microsoft Corporation. It is disclosed pursuant to a non-disclosure agreement between the recipient and Microsoft. This document is provided for informational purposes only and Microsoft makes no warranties, either express or implied, in this document. Information in this document, including URL and other Internet Web site references, is subject to change without notice. The entire risk of the use or the results from the use of this document remains with the user. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2008 Microsoft Corporation. All rights reserved.

Active Directory, Microsoft, MS-DOS, Visual Basic, Visual Studio, Windows, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.

Contents

[Online Responder Installation, Configuration, and Troubleshooting Guide 7](#_Toc206567636)

[Overview 7](#_Toc206567637)

[Understanding Revocation Checking Concepts 7](#_Toc206567638)

[CRLs 8](#_Toc206567639)

[OCSP 8](#_Toc206567640)

[Understanding the Online Responder's Components 9](#_Toc206567641)

[OCSP Client 9](#_Toc206567642)

[Online Responder Web Proxy Cache 11](#_Toc206567643)

[Online Responder Service 11](#_Toc206567644)

[Revocation Configuration 12](#_Toc206567645)

[Revocation Providers 12](#_Toc206567646)

[Exploring Online Responder Deployment Models 12](#_Toc206567647)

[Achieving Scalability and High Availability 13](#_Toc206567648)

[Deployment Models for Extranet Scenarios 13](#_Toc206567649)

[Deploying Microsoft Online Responder 15](#_Toc206567650)

[Installing the Online Responder Service 15](#_Toc206567651)

[Preparing the Environment 22](#_Toc206567652)

[Configuring the CAs 22](#_Toc206567653)

[Configuring the OCSP Response Signing certificate template 24](#_Toc206567654)

[Configuring the OCSP Response Signing certificate template when using a Windows Server 2008–based CA 25](#_Toc206567655)

[Configuring the OCSP Response Signing certificate template when using a Windows Server 2003–based CA 26](#_Toc206567656)

[Configuring OCSP Response Signing template permissions when using a Windows Server 2008 or Windows Server 2003–based CA 27](#_Toc206567657)

[Assigning an OCSP Response Signing template to a CA 28](#_Toc206567658)

[Enrolling for an OCSP Response Signing certificate 28](#_Toc206567659)

[Renewing OCSP Response Signing certificates 29](#_Toc206567660)

[Enrolling for an OCSP Response Signing certificate against a stand-alone CA 31](#_Toc206567661)

[Using a hardware security module (HSM) to protect OCSP signing keys 31](#_Toc206567662)

[Modifying the Online Responder service credentials 32](#_Toc206567663)

[Configuring the OCSP Response Signing template 32](#_Toc206567664)

[Configuring the Online Responder 32](#_Toc206567665)

[Configuring Online Responder properties 33](#_Toc206567666)

[Web proxy settings 33](#_Toc206567667)

[Audit settings 34](#_Toc206567668)

[Security settings 36](#_Toc206567669)

[Managing revocation configurations 36](#_Toc206567670)

[Creating a revocation configuration 36](#_Toc206567671)

[Modifying a revocation configuration 41](#_Toc206567672)

[Managing Array members 44](#_Toc206567673)

[Adding Array members 44](#_Toc206567674)

[Monitoring and managing Array members 45](#_Toc206567675)

[Enabling Remote Management 45](#_Toc206567676)

[Planning for CA Certificate Renewal 46](#_Toc206567677)

[Understanding Revocation Configuration and CA Certificate Relationship 46](#_Toc206567678)

[Creating Revocation Configuration for Renewed CA 47](#_Toc206567679)

[Performing Online Responder Backup and Restore 47](#_Toc206567680)

[Performing Online Responder Migration 48](#_Toc206567681)

[Troubleshooting the Online Responder 48](#_Toc206567682)

[Online Responder Service Problems 48](#_Toc206567683)

[Online Responder Snap-In Messages 59](#_Toc206567684)

[Array Configuration messages 59](#_Toc206567685)

[Revocation Configuration messages 61](#_Toc206567686)

[Enabling CryptoAPI 2.0 Diagnostics 63](#_Toc206567687)

[Additional Resources 64](#_Toc206567688)

# Online Responder Installation, Configuration, and Troubleshooting Guide

Note

To download a copy of this document, see <http://go.microsoft.com/fwlink/?LinkId=85461>.

## Overview

Public key infrastructure (PKI) consists of multiple components, including certificates, certificate revocation lists (CRLs), and certification authorities (CAs). In most cases, applications that depend on X.509 certificates, such as Secure/Multipurpose Internet Mail Extensions (S/MIME), Secure Sockets Layer (SSL), and smart cards, are required to validate the status of the certificates used when performing authentication, signing, or encryption operations. The certificate status and revocation checking is the process by which the validity of certificates is verified based on two main categories: time and revocation status.

 Time. Certificates are issued for a fixed period of time and considered valid as long as the expiration date of the certificate is not reached, unless revoked before that date.

 Revocation status. Certificates can be revoked before their expiration date because of multiple reasons such as key compromise or suspension. Before performing any operation, applications often validate that the certificate was not revoked.

Although validating the revocation status of certificates can be performed in multiple ways, the common mechanisms are CRLs, delta CRLs, and Online Certificate Status Protocol (OCSP) responses. Common scenarios for using OCSP include:

 SSL/Transport Layer Security (TLS) certificate revocation checking

 Smart card logon

 Enterprise S/MIME

 Extensible Authentication Protocol (EAP)/TLS–based virtual private network (VPN)

Microsoft natively supports only CRL in operating systems prior to the Windows Vista® operating system. Windows Vista and the Windows Server® 2008 operating system will natively support both CRL and OCSP as a method of determining certificate status. The OCSP support includes both the client component as well as the Online Responder, which is the server component.

## Understanding Revocation Checking Concepts

When an application performs a certificate evaluation, the validation is performed on all certificates in that certificate's chain. This includes every certificate from the end-entity certificate presented to the application to the root certificate.

When the first certificate in the chain is validated, the following process takes place:

1. The certificate chaining engine attempts to build the chain for the certificate inspected by querying the local certificate store or by downloading from one of the URLs available in the inspected certificate's authority information access extensions.

2. For all certificate chains that end in a trusted root, all certificates in the chain are validated. This involves the following steps:

 Verify that each certificate's signature is valid.

 Verify that the current date and time fall within each certificate's validity period.

 Verify that each certificate is not corrupt or malformed.

3. Each certificate in the certificate chain is checked for revocation status. Revocation checking is performed either by using a CRL or OCSP, based on the certificate configuration.

After the validation check is completed, the certificate chaining engine returns the results of the validation check to the application that originated the validation request. The results will indicate if all certificates in the chain are valid, if the chain terminates at a non-trusted root CA, if any certificates in the chain are not valid, or if the revocation status for any of the certificates in the chain cannot be determined.

For more information, see Certificate Revocation and Status Checking (<http://go.microsoft.com/fwlink/?LinkID=27081>).

### CRLs

A CRL is a file, created and signed by a CA, that contains serial numbers of certificates that have been issued by that CA and are revoked. In addition to the serial number for the revoked certificates, the CRL also contains the revocation reason for each certificate and the time the certificate was revoked.

Currently, two types of CRLs exist: base CRLs and delta CRLs. Base CRLs maintain a complete list of revoked certificates while delta CRLs maintain only those certificates that have been revoked since the last publication of a base CRL.

The major drawback of CRLs is their potentially large size, which limits the scalability of the CRL approach. The large size adds significant bandwidth and storage burdens to the CA and relying party, and therefore limits the ability of the system to distribute the CRL. Bandwidth, storage space, and CA processing capacity can also be negatively affected if the publishing frequency gets too high. Numerous attempts have been made to solve the CRL size issue through the introduction of partitioned CRLs, delta CRLs, and indirect CRLs. All these approaches have added complexity and cost to the system without providing an ideal solution to the underlying problem.

Another drawback of CRLs is latency; because the CRL publishing period is predefined, information in the CRL might be out of date until a new CRL or delta CRL is published.

### OCSP

OCSP is a Hypertext Transfer Protocol (HTTP) that allows a relying party to submit a certificate status request to an OCSP responder. This returns a definitive, digitally signed response indicating the certificate status. The amount of data retrieved per request is constant regardless of the number of revoked certificates in the CA. Most OCSP responders get their data from published CRLs and are therefore reliant on the publishing frequency of the CA. Some OCSP responders can, however, receive data directly from the CA's certificate status database and consequently provide near real-time status.

Scalability is the major drawback of the OCSP approach. Since it is an online process and is designed to respond to single certificate status requests, it results in more server hits, requiring multiple and sometimes geographically dispersed servers to balance the load. The response signing and signature verification processes also take time, which can adversely affect the overall response time at the relying party. Finally, since the integrity of the signed response depends on the integrity of the OCSP responder's signing key, the validity of this key must also be verified after a response is validated by the client.

## Understanding the Online Responder's Components

The Microsoft OCSP implementation is divided into client and server components (Figure 1). The client component is built into the CryptoAPI 2.0 library while the server component is introduced as a new service provided by the Active Directory® Certificate Services (AD CS) server role.

Figure 1: Microsoft Online Responder Components



### OCSP Client

The OCSP client is fully integrated into the CryptoAPI 2.0 certificate revocation infrastructure. It implements the recommendation specified in the draft Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (PKIX) "Lightweight OCSP Profile for High Volume Environment" and is optimized for high-volume scenarios.

The major difference between the Lightweight OCSP Profile and RFC 2560, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP," can be summarized as follows:

 The Lightweight OCSP Profile supports both the Hypertext Transfer Protocol (HTTP) and Secure Hypertext Transfer Protocol (HTTPS).

 Lightweight OCSP Profile responses must specify notBefore and notAfter dates, which are not required in the full profile.

 Signed requests are not supported in the Lightweight OCSP Profile. The client cannot create a signed request; if a signed request, which can be created by third-party OCSP clients, is sent to the Online Responder an "Unauthorized" response is returned.

 With the Lightweight OCSP Profile, nonce is not supported in the request and ignored in the response. However, the Online Responder supports the nonce extension and will return a response that includes the nonce extension if configured to do so. For more information, see [Managing revocation configurations](#DSDOC_BKMK_ManagingRevocationConfigurati).

When an application calls CryptoAPI 2.0 to verify a certificate that specifies locations to Online Responders, the revocation infrastructure performs the following basic steps (for each Online Responder specified in the authority information access extension):

1. Search the local CryptoAPI 2.0 in-memory and disk caches to find a cached OCSP response that has a valid time. The disk cache is located at: <drive>:\Users\<User name>\AppData\LocalLow\Microsoft\CryptnetUrlCache.

Note

By default, response caching is performed by the OCSP client. This behavior can be changed by modifying the ChainCacheResynchFiletime value located in the HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config registry key. The ChainCacheResynchFiletime value specifies the date and time to clear the in-memory cache. The following Certutil commands can be used to modify the ChainCacheResynchFiletime value:

 To set a registry value to the current date and time:

certutil –setreg chain\ChainCacheResyncFiletime @now

 To set a registry value to the current date and time plus 3 days and 1 hour:

certutil –setreg chain\ChainCacheResyncFiletime @now+3:1

 To display a registry value:

certutil –getreg chain\ChainCacheResyncFiletime

 To delete a registry value:

certutil –delreg chain\ChainCacheResyncFiletime

2. If no acceptable cached response can be found, a request is sent by using the HTTP GET method. In situations where the Online Responder does not support the GET method, CryptoAPI 2.0 will retry the request by using the HTTP POST method. Only one certificate can be validated per OCSP request. Moreover, it is not possible to configure CryptoAPI 2.0 to always try the POST method first.

3. The signature on the response, including the delegated OCSP signer certificate, is verified. If the certificate contains the id-pkix-ocsp-nocheck extension, identified by the object identifier 1.3.6.1.5.5.7.48.1.5, CryptoAPI will not verify the revocation status of the delegated OCSP signer certificate.

### Online Responder Web Proxy Cache

The Online Responder Web proxy cache represents the service interface for the Online Responder. It is implemented as an Internet Server Application Programming Interface (ISAPI) extension hosted by Internet Information Services (IIS), and it performs the following operations:

 Request decoding. All requests sent to the Online Responder are Abstract Syntax Notation One (ASN.1)–encoded according to the request/response schema defined in RFC 2560. For more information about RFC 2560, see RFC 2560, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP" (<http://go.microsoft.com/fwlink/?LinkID=71068>). After a request is received by the Online Responder Web proxy, the decoder component will try to decode the request and extract the certificate serial number to be validated.

 Response caching. After a request is received and a certificate serial number is extracted, the Online Responder Web proxy will check the local cache for a valid response. The cache is implemented as part of the ISAPI extension and is an in-memory cache. If a client request generates a cache fault, the Online Responder Web proxy will make a request to the Online Responder service for a response. The cache item validity period is set to the CRL validity period from which the response was generated or to the signing key validity, whichever is shorter.

Note

In addition to the OCSP ISAPI extension caching, the IIS HTTP.SYS library performs caching for 120 seconds. Multiple requests to the Online Responder in that time period will be served with the HTTP.SYS-cached response.

### Online Responder Service

The Online Responder is a Microsoft Windows NT® service (ocspsvc.exe) that is running with Network Service privileges. It performs the following operations:

 Manages the Online Responder configuration. The Online Responder provides a responder-wide set of attributes that can be configured. These attributes include public interfaces, access control settings, audit settings, and Web proxy cache settings. All the configuration information is stored in the registry under HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\OCSPSvc\Responder.

 Retrieves and caches revocation information based on configuration. Based on the revocation configuration, the Online Responder service can retrieve and cache revocation information such as CRLs and delta CRLs for future use. For more information, see [Revocation Configuration](#DSDOC_BKMK_RevocationConfiguration045d2a).

 Signs responses. For each successful request, the Online Responder signs the response with a pre-acquired signing key.

 Audits configuration changes. To conform to the Common Criteria requirements, all configuration changes of the Online Responder can be audited. For more information about audit settings, see [Configuring the Online Responder](#DSDOC_BKMK_ConfiguringtheOnlineResponder).

### Revocation Configuration

A revocation configuration is a set of definitions that configure the Online Responder service to respond to a certificate status request for a specific CA. Every Online Responder can have one or more revocation configurations. Revocation configurations include:

 CA certificate

 Signing certificate for OCSP responses

 Revocation provider–specific configuration

### Revocation Providers

Revocation providers are the components that are responsible for retrieving and caching revocation information that is used by the Online Responder service. When the Online Responder service receives an OCSP request, it first locates the revocation configuration, which is configured to provide revocation information for the CA that issued the certificate in question. After located, the Online Responder service extracts the certificate serial number and searches a local CRL. (For more information about the local CRL, see [Managing revocation configurations](#DSDOC_BKMK_ManagingRevocationConfigurati).) If no relevant information is found, the Online Responder service sends the serial number to the revocation provider, which is used by that revocation configuration. The provider, in turn, returns the status of the certificate to the Online Responder service.

Although the revocation providers were designed for extensibility to allow custom providers to be developed and used by the Online Responder, the Windows Server 2008 Online Responder provides only a default CRL-based revocation provider and does not allow new providers to be added.

## Exploring Online Responder Deployment Models

When deploying the Online Responder, different deployment models should be considered for scalability, high availability, and security reasons.

### Achieving Scalability and High Availability

Figure 2 shows the deployment models that can provide scalability and high availability. The Online Responder can be deployed on a single computer or on a software cluster that contains one or more computers. Clustering can be achieved by using any software or hardware TCP/IP load balancers. The Online Responder Microsoft Management Console (MMC) snap-in provides the ability to manage multiple responders as if they were a single entity. For more information, see [Configuring the Online Responder](#DSDOC_BKMK_ConfiguringtheOnlineResponder).

Figure 2: Scalability and High Availability Deployment Models



### Deployment Models for Extranet Scenarios

When deploying extranet-facing Online Responders, one of the design considerations is the level of protection provided for the Online Responder signing key. Figure 3 shows two options for protecting the Online Responder.

Figure 3: Extranet Deployment Models



In diagram 1 of Figure 3, the Online Responder is located in a protected local area network (LAN), while all requests are redirected by an authenticated server that is running IIS, which is located in a perimeter network (also known as DMZ, demilitarized zone, and screened subnet). The advantage of such a deployment model is that the firewall configuration requires only pass-through for port 80 between IIS and the Online Responder. Similar results can be achieved by using the reverse-proxy capability of Microsoft Internet Security and Acceleration (ISA) Server as demonstrated in diagram 2 of Figure 3. To configure ISA Server 2006 Web publishing rules, use the following steps:

1. Open the Microsoft Internet Security and Acceleration Server 2006 snap-in. Right-click the Firewall Policy node, point to New, and click Web Site Publishing Rule.

2. Enter a name for the new rule, and click Next.

3. Verify that Allow is selected, and click Next.

4. If you are targeting a single server or a Network Load Balancing (NLB) cluster, click Publish a single Web site or load balancer. If you are using ISA Server as the load balancer for an Online Responder Array, click Publish a server farm of load balanced Web servers. Click Next.

5. Click Use non-secured connections to connect the published Web server or server farm, and click Next.

Note

SSL should not be used with OCSP.

6. Type the name that clients use to connect to the Online Responder. This is either the computer name of the server running ISA Server or a DNS alias that is set up to point to the server running ISA Server.

7. To limit the publishing rule to only forward OCSP requests, type ocsp/\* in the Path box.

8. If you are using ISA Server as the load balancer, either select an existing server farm or create a new server farm.

9. To create a new server farm, click New to start the New Server Farm Wizard. Enter a name for the new server farm, and click Next.

10. Click Add to add servers by name or IP address.

11. Leave the default connectivity monitoring settings, and click Next.

12. Click Finish to close the wizard.

13. In the Public name box, enter the fully qualified domain name (FQDN) or IP address to be used for the Online Responder.

14. In the Web listener list, click a Web listener. If a Web listener is not already set up, click New to start the New Web Listener Wizard.

15. Enter a name for the Web listener, and click Next.

16. Click Do not require SSL secured connections with clients.

Note

SSL should not be used with OCSP.

17. Select the All Networks (and Local Host) check box to allow all network computers to connect to the Online Responder service, and click Next.

18. In the Select how clients will provide credentials to ISA Server list, click No Authentication, and then click Next.

Note

The Online Responder service is meant for anonymous access.

19. Click Next.

Note

Since no authentication settings are provided, there are no single sign-on settings to configure.

20. Click Finish to close the wizard.

21. On the Select Web Listener page, click Next.

22. On the Authentication Delegation page, click Next.

23. On the User Sets page, click Next.

24. Click Finish to close the wizard.

25. After the wizard is finished, click Apply to enable the new policy.

26. After the rules are applied, click OK to close the dialog box.

## Deploying Microsoft Online Responder

Deploying the Online Responder consists of three steps:

 Install the Online Responder service.

 Prepare the environment.

 Configure the Online Responder.

### Installing the Online Responder Service

Deploying Online Responders should occur after deploying CAs and before deploying the end-entity certificates. For more information about Server Manager and CA deployment, see Windows Server 2008 CA Enhancements ([http://go.microsoft.com/fwlink/?LinkID=83212](http://go.microsoft.com/fwlink/?LinkID=27081)).

1. Click Start, point to Administrative Tools, and then click Server Manager.

Figure 4: Server Manager



2. If the Online Responder is being installed on a computer without any other AD CS role services, click Add roles on the main page.

Note

If the Online Responder is installed on a computer where the CA or one of its components is already installed, select the Active Directory Certificate Services node in the left pane, and then click Add role services on the main page.

3. On the Select Server Roles page of the Add Roles Wizard (Figure 5), select the Active Directory Certificate Services check box, and then click Next.

Figure 5: Select Server Roles



4. On the Select Role Services page (Figure 6), select the Online Certificate Status Protocol check box.

Figure 6: Select Role Services



Because the Online Responder requires IIS, you are prompted to install IIS role services (Figure 7). The following IIS features are required for the Online Responder to operate properly:

Web Server

Common HTTP Features

 Static Content

 Default Document

 Directory Browsing

 Http Errors

 Http Redirection

Application Development

 .NET Extensibility

 ISAPI Extensions

Health and Diagnostics

 Http Logging

 Logging Tools

 Request Monitor

 Tracing

Security

 Request Filtering

Performance

 Static Content Compression

Management Tools

 IIS Management Console

 IIS 6 Management Compatibility

 IIS Metabase Compatibility

5. Click Add Required Role Services to install the required IIS services, and click Next.

Figure 7: Add Required Role Services



6. The next two steps allow selecting the role services for the Web server (IIS). Click Next twice.

7. On the Confirm Installation Options page (Figure 8), click Install.

Figure 8: Confirm Installation Options



Note

The IIS installation process might take a long time to complete.

Figure 9: Installation Progress



8. When the installation is complete, the status of the installation process is displayed on the Installation Results page.

Figure 10: Installation Results



9. Click Close.

As part of the setup process, a virtual directory named OCSP is created in IIS, and the ISAPI extension used as the Web proxy is registered. You can manually register or un-register the Web proxy by using either of the following commands:

certutil –vocsproot

certutil –vocsproot delete

### Preparing the Environment

The environment preparation consists of the following steps:

 Configure the CA.

 Configure the OCSP Response Signing certificate template.

 Enroll for an OCSP Response Signing certificate against a stand-alone CA.

 Use a hardware security module (HSM) to protect OCSP signing keys.

#### Configuring the CAs

You must configure the CAs to include the Online Responder's URL as part of the authority information access extension of issued certificates. This URL is used by the OCSP client to validate the certificate status.

To configure the authority information access extension

|  |
| --- |
| 1. Open the Certification Authority snap-in, right-click the name of the issuing CA,and then click Properties.2. Click the Extensions tab.3. In the Select extension list, click Authority Information Access (AIA) (Figure 11), and then click Add.Figure 11: CA Properties4. In the Add Location dialog box (Figure 12), type the full URL of the Online Responder, which should be in the following form: http://<DNSServerName>/<vDir> Note When installing the Online Responder, the default virtual directory used in IIS is OCSP.Figure 12: Add Location dialog box5. Click OK.6. Select the location from the Location list. 7. Select the Include in the online certificate status protocol (OCSP) extension check box, and then click OK. |

#### Configuring the OCSP Response Signing certificate template

The Online Responder can sign OCSP responses by using the issuing CA key or a dedicated signing key. A signing certificate has the following attributes:

 Has a short validity period. (A validity period of two weeks is recommended.)

 Includes the id-pkix-ocsp-nocheck extension.

 Does not include CRL distribution point and authority information access extensions.

 Includes id-kp-OCSPSigning enhanced key usage (EKU).

 The steps to configure the OCSP Response Signing template in the Windows Server 2003 operating system are different from the steps in Windows Server 2008.

Note

In Windows Server 2008, a version 3 template is introduced. The new template version allows advanced cryptography support in addition to other enhancements. For more information, see Windows Server 2008 CA Enhancements ([http://go.microsoft.com/fwlink/?LinkID=83212](http://go.microsoft.com/fwlink/?LinkID=27081)).

##### Configuring the OCSP Response Signing certificate template when using a Windows Server 2008–based CA

In Windows Server 2008, a new certificate template is added to the available templates in Active Directory Domain Services (AD DS). The new template, named OCSP Response Signing, is a version 3 template preconfigured with the required extensions and attributes listed previously. No modifications are required to the template or to the CA.

Figure 13 illustrates the flow that determines the behavior of the policy module in Windows Server 2008 when processing a request for the OCSP Response Signing certificate.

Figure 13: OCSP Response Signing Certificate Request Processing



The EDITF\_ENABLEOCSPREVNOCHECK flag is a new CA registry flag introduced in the Windows Server 2008–based CA. The new flag, which is not enabled by default, allows the CA policy module to issue certificates that include the id-pkix-ocsp-nocheck extension. The new OCSP Response Signing template includes an additional flag as well, named CT\_FLAG\_ADDREVNOCHECK, which instructs the policy module to add the id-pkix-ocsp-nocheck extension. If either the EDITF\_ENABLEOCSPREVNOCHECK flag is enabled or the template includes the CT\_FLAG\_ADDREVNOCHECK flag, the policy module will search for an OCSP Signing EKU in the request and in the template. If both conditions are met, the policy module will add the id-pkix-ocsp-nocheck extension and will remove the authority information access and CRL distribution point extensions from the certificate. This flow allows the Windows Server 2008–based CA to issue an OCSP Response Signing certificate from an enterprise CA as well as from a stand-alone CA.

If an enterprise CA is used, no additional configuration is required except for enabling the CA to issue certificates based on the OCSP Response Signing template. If a stand-alone CA is used, the following commands should be used to enable or disable the EDITF\_ENABLEOCSPREVNOCHECK flag on the CA.

To enable the flag, run the following command:

certutil -v -setreg policy\editflags +EDITF\_ENABLEOCSPREVNOCHECK

To disable the flag, run the following command:

certutil –v –setreg policy\editflags –EDITF\_ENABLEOCSPREVNOCHECK

After enabling or disabling the flag, the CA should be restarted for the changes to take effect.

##### Configuring the OCSP Response Signing certificate template when using a Windows Server 2003–based CA

One of the drawbacks of certificate templates is the inability to add custom extensions. This introduces a problem creating and configuring the OCSP Response Signing template in Windows Server 2003 and the ability to add the id-pkix-ocsp-nocheck extension. The following procedures enable you to use the OCSP Response Signing template with a Windows Server 2003 CA.

To configure the certificate template for use with a Windows Server 2003 CA

|  |
| --- |
| 1. Open the Certificate Templates snap-in.Note The snap-in must be opened from within Windows Server 2008. This is required because only the new version of the snap-in supports the new version 3 templates and allows the duplication of version 3 templates.2. Right-click the OCSP Response Signing template, and then click Duplicate. The Duplicate Template dialog box (Figure 14) appears.Figure 14: Duplicate Template dialog box3. Click Windows 2003 Server, Enterprise Edition, and then click OK. This will create a version 2 template, which can be issued by the Windows Server 2003–based CA and still include the id-pkix-ocsp-nocheck extension. |

Next, it is necessary to configure the CA to allow custom extensions to be included in certificate requests.

To configure the Windows Server 2003 CA

|  |
| --- |
| 1. On the CA computer, open a command prompt and type the following command:certutil -v -setreg policy\EnableRequestExtensionList +1.3.6.1.5.5.7.48.1.52. Restart the CA service by typing the following commands:net stop certsvcnet start certsvc |

The CA is now configured to issue OCSP Response Signing certificates.

##### Configuring OCSP Response Signing template permissions when using a Windows Server 2008 or Windows Server 2003–based CA

As with any template, the enrollment permissions for Read, Enroll, AutoEnroll, Write, and Full Control must be configured.

To configure the template security settings to allow Online Responders to enroll for signing certificates

|  |
| --- |
| 1. Open the Certificate Templates snap-in.2. Double-click the OCSP Response Signing template or a duplicate you have created, and then click the Security tab.3. Add the Online Responder computers to the Group or user names list.4. To allow Online Responder computers to enroll for the OCSP Response Signing certificate, select the Allow check box for the Read and Enroll permissions.  |

Note

The Autoenroll permission is not used by the Online Responder, which has a separate implementation of autoenrollment that is explained in detail later in this document. The default Windows autoenrollment implementation limits a template to issuing one certificate per client. By default, Windows autoenrollment will renew only one of the signing certificates available on the Online Responder computer and will archive the rest. In some cases, Windows autoenrollment will not use the original CA that issued the certificate for renewal. This is not the behavior expected by the Online Responder, which requires renewal by the same CA.

#### Assigning an OCSP Response Signing template to a CA

After the templates are properly configured, the CA needs to be configured to issue that template.

To configure the CA to issue certificates based on the newly created OCSP Response Signing template

|  |
| --- |
| 1. Open the Certification Authority snap-in.2. Right-click Certificate Templates, click New, and then click Certificate Template to Issue.3. In the available templates list, click the OCSP Response Signing template, and then click OK. |

#### Enrolling for an OCSP Response Signing certificate

For enhanced security, the Online Responder runs with Network Service privileges. This means it does not have access to computer private keys by default, and permissions for private keys that need to be accessed by the Online Responder have to be modified to allow access. A new functionality, which is introduced in version 3 templates, allows the enrollment client to configure permissions for computer keys as part of the enrollment process to allow access for services running as Network Service. This functionality is available only in Windows Vista and Windows Server 2008.

The new OCSP Response Signing version 3 template enables this functionality by default, allowing the enrollment client to modify the private key permissions automatically to allow Network Service Read access to the OCSP signing private key.

As long as a Windows Server 2008–based CA is used to issue a certificate based on the OCSP Response Signing template or a duplicate of that template, no additional configuration is required.

If a Windows Server 2003, Enterprise Edition–based CA is used, OCSP signing private key permissions must be configured manually on the Online Responder computer to allow the Online Responder service access to the private key.

In Windows Vista and Windows Server 2008, the ability to modify private key permissions was added to the Certificates snap-in.

The following procedure is required only if a Windows Server 2003–based CA is used to issue OCSP signing certificates.

To configure the private key permissions for an OCSP signing certificate issued by a Windows Server 2003–based CA

|  |
| --- |
| 1. On the Online Responder computer, open the Certificates snap-in for the local computer.2. In the available certificates list, select the OCSP Response Signing certificate. Note The signing certificate should first be manually enrolled.3. On the Actions menu, point to All Tasks, click Manage Private Keys, and then click Add.4. Type network service, and then click OK.5. Verify that only the Read permission is allowed for the NETWORK SERVICE, and then click OK.6. Restart the Online Responder service by typing the following commands at a command prompt:net stop ocspsvcnet start ocspsvc |

Note

The steps above apply only if the Online Responder revocation configuration is set for manual enrollment of the OCSP signing certificate. If the revocation configuration is configured for OCSP automatic enrollment, the private keys should have the correct permissions by default and the steps above should not be required.

Note

If the revocation configuration is set to use OCSP autoenrollment and a Windows Server 2003–based CA is used, renewal of OCSP signing certificates will require additional steps, as specified below.

#### Renewing OCSP Response Signing certificates

After the initial certificate enrollment is complete and the proper key access control list (ACL) is set, renewing OCSP Response Signing certificates is similar to any other certificate renewal procedure with one caveat. This caveat is to follow the correct procedure to renew the OCSP Response Signing certificate during the period between the time the CA certificate was renewed to the expiration date of the renewed CA certificate. The problem arises because the same CA key that was used to sign issued certificates must be used to sign the OCSP Response Signing certificates. Since this key is no longer available on the CA, no signing certificates can be issued.

Figure 15 illustrates the problem. OCSP Response Signing certificates (S1, S2) need to be signed by the same key (k1) that was used to sign the end-entity certificates (C1, C2) that they provide status for. After the CA key is renewed (t1), the CA will be using the new key (k2) to sign new issued certificates. In the period between the time the CA certificate was renewed (t1) to the expiration date of the renewed CA certificate (t2), the CA cannot issue or renew OCSP Response Signing certificates, which can be used to sign OCSP responses for existing valid certificates (C1, C2).

Figure 15: The OCSP Response Signing certificate renewal problem



To overcome this limitation, the Windows Server 2008–based CA was updated to allow the renewal of OCSP Response Signing certificates by using existing keys. This feature is not enabled by default. Use the following procedure to allow the renewal of OCSP Response Signing certificates by using existing CA keys.

To allow the renewal of OCSP Response Signing certificates by using existing CA keys

|  |
| --- |
| 1. On the CA computer, open a command prompt, and type: certutil -setreg ca\UseDefinedCACertInRequest 1 2. Press ENTER.3. Restart the CA service. |

When using a Windows Server 2003–based CA, it is impossible to renew OCSP Response Signing certificates after the CA certificate was renewed. To overcome this limitation, issue n OCSP signing certificates for each Online Responder computer from the Windows 2003–based CA, where n = (the number of weeks until the expiration date of the CA key)/2.

Note

This procedure must be performed before renewing the CA certificate.

Each of the issued certificates should have a validity period of two weeks longer than the previous one. For example:

 Signing Certificate 1: Valid from NOW until Now+2 weeks

 Signing Certificate 2: Valid from NOW until Now+4 weeks

 Signing Certificate 3: Valid from NOW until Now+6 weeks

The Online Responder service will select the signing certificate with the shorter validity period first and will use that certificate until it expires.

#### Enrolling for an OCSP Response Signing certificate against a stand-alone CA

Since stand-alone CAs do not support the version 2 or version 3 certificate template required to create an OCSP Response Signing certificate, you must manually create and submit an OCSP Response Signing certificate request. Use the following procedure to enroll for an OCSP Response Signing certificate against a stand-alone CA.

To enroll for an OCSP Response Signing certificate against a stand-alone CA

|  |
| --- |
| 1. Click Start, point to All Programs, click Accessories, and then click Notepad.2. Copy and paste the following request data into Notepad:[NewRequest] Subject = "CN=testca,O=Contoso,OU=nt" PrivateKeyArchive = FALSE Exportable = TRUE UserProtected = FALSE MachineKeySet = TRUE ProviderName = "Microsoft Enhanced Cryptographic Provider v1.0" UseExistingKeySet = FALSE RequestType = PKCS10[EnhancedKeyUsageExtension] object identifer="1.3.6.1.5.5.7.3.9"[Extensions] 1.3.6.1.5.5.7.48.1.5 = Empty3. Save the file as ocsp.inf.4. Close Notepad.5. At a command prompt, type:certreq.exe –New ocsp.inf ocsp.reqcertreq.exe –Submit ocsp.req ocsp.cercertreq.exe –Accept ocsp.cer |

After the enrollment process is complete, you must modify the ACL of the private key to allow the Online Responder service to access the private key. For the required steps to configure private key permissions, see [Configuring the OCSP Response Signing certificate template](#DSDOC_BKMK_ConfiguringtheOCSPResponseSig).

#### Using a hardware security module (HSM) to protect OCSP signing keys

The following configuration steps are required in case an HSM (or a smart card) is used to protect the OCSP signing keys.

##### Modifying the Online Responder service credentials

The Online Responder service uses Network Service credentials by default. To allow the Online Responder service to interact with an HSM, it is required to change the service credentials to Local System. Use the following steps to configure the Online Responder service credentials.

To configure the Online Responder service credentials

|  |
| --- |
| 1. Open the Services snap-in.2. Right-click the Online Responder service, and click Properties.3. Click the Log On tab.4. Click the Local System account.5. Select the Allow service to interact with desktop check box, and click OK. |

##### Configuring the OCSP Response Signing template

When you use an HSM to protect the OCSP signing keys, you must also configure the OCSP Response Signing template to use the HSM's CryptoAPI cryptographic service provider (CSP) or Cryptography Next Generation (CNG) provider. If only a CryptoAPI CSP is available, you must duplicate the version 3 OCSP Response Signing template and create a new version 2 template that supports CryptoAPI CSPs. See "Configuring the OCSP Response Signing certificate template when using the Windows Server 2003–based CA" in the [Configuring the OCSP Response Signing certificate template](#DSDOC_BKMK_ConfiguringtheOCSPResponseSig) section for the required steps to create a version 2 template.

### Configuring the Online Responder

Whether the Online Responder is deployed on a single computer, clustered array, or multiple clustered arrays, the Online Responder management tools provide a single point of monitoring and configuration for Online Responder deployment.

The management tools installed by default on all Windows Server 2008 versions include the Online Responder snap-in (Figure 16), which provides all the required functionality for managing an Online Responder.

Figure 16: Online Responder snap-in



The Online Responder console tree includes the following views:

 Online Responder. This view provides general information about the Online Responder configuration status and allows configuring of Online Responder properties.

 Revocation Configuration. This view allows adding, modifying, and deleting revocation configurations. For more information about revocation configurations, see [Managing revocation configurations](#DSDOC_BKMK_ManagingRevocationConfigurati).

 Array Configuration. This view allows configuring, monitoring, and troubleshooting Online Responder Array members. For more information about Array configurations, see [Managing Array members](#DSDOC_BKMK_ManagingArraymembers045d2a97_).

#### Configuring Online Responder properties

The Online Responder provides a set of configurable properties that are Online Responder–wide and apply to the Online Responder's service operation.

To open the Online Responder dialog box, click Responder Properties on the Action menu or click Responder Properties in the Action pane.

##### Web proxy settings

The Online Responder Web proxy cache is implemented as an ISAPI extension hosted by IIS. The following configurable settings are enabled (Figure 17).

 Web proxy threads. This setting refers to the number of threads that will be allocated by the Online Responder ISAPI extension for handling requests. Increasing the number of threads will use more of the server's memory and reducing the number of threads will reduce the number of clients that can be served concurrently. The minimum thread number allowed is five.

 Cache entries allowed. The cache is implemented as part of the Online Responder's ISAPI extension and is an in-memory cache only. The recommended cache size is between 1,000 and 10,000 entries. A small cache size will cause more cache faults and will result in a higher load on the Online Responder service for lookup and signing operations; a large cache size will increase the Online Responder's memory usage. If the CA certificate is used to sign responses, the size of the cache entries in memory is approximately 200 bytes; if a delegated signer certificate is used to sign responses, the size of the cache entries in memory is approximately 2 KB (assuming a key size of 1,024 bytes).

Figure 17: Web proxy settings



##### Audit settings

To comply with Common Criteria requirements for secure certificate issuance systems and to provide a secure platform, certain event and configuration settings are logged to the Windows security event log. The Online Responder allows the configuration of the following audit events (Figure 18).

 Start/Stop the Online Responder Service. Every Start/Stop event of the Online Responder service will be logged.

 Changes to the Online Responder configuration. All Online Responder configuration changes, including audit settings changes, will be logged.

 Changes to the Online Responder security settings. All changes to the Online Responder service request and management interfaces ACL will be logged.

 Requests submitted to the Online Responder. All requests processed by the Online Responder service will be logged. This option can create a high load on the service and should be evaluated on a case-by-case basis. Note that only requests that require a signing operation by the Online Responder will generate audit events; requests for previously cached responses will not be logged.

Figure 18: Audit settings



Audit events will be logged to the Windows security log only if the Audit object access policy is enabled.

To enable the Audit object access policy

|  |
| --- |
| 1. Open the Local Group Policy Editor.2. Under Computer Configuration, expand Windows Settings, Security Settings, and Local Policies, and then click Audit Policy.3. Double-click the Audit object access policy.4. Select the Success and Failure check boxes, and click OK. |

##### Security settings

The security settings for the Online Responder include two permission entries that can be set for users and services to allow or deny access to the request and administration interfaces.

 Manage Online Responder. The Online Responder exposes a management interface (IOCSPAdmin) that provides the ability to perform administrative tasks such as creating and managing revocation configurations and to modify the Online Responder's global settings.

 Proxy Requests. The Online Responder exposes a request interface (IOCSPRequestD) that allows the Online Responder Web proxy component to submit requests for certificate status to the Online Responder service. This interface is not used by applications that submit the OCSP request.

#### Managing revocation configurations

Revocation configurations include a set of definitions that enable the Online Responder to provide a signed OCSP response. These definitions include the CA certificate, the signing certificate, and the source of the revocation information. Each revocation configuration serves requests for a specific CA key pair and certificate. The following rules apply:

 A separate revocation configuration should be created for each CA that was configured to include the Online Responder authority information access in issued certificates.

 A separate revocation configuration should be created for each CA that is renewed with a new key pair.

The Revocation Configuration view allows adding, modifying, and deleting revocation configurations.

##### Creating a revocation configuration

This section explores the process of creating, modifying, and deleting revocation configurations.

To create a revocation configuration

|  |
| --- |
| 1. On the Action menu or in the Actions pane, click Add Revocation Configuration. The Add Revocation Configuration wizard appears.2. Click Next. 3. In the Name box of the Name the Revocation Configuration page, enter a friendly name for the revocation configuration (which will help identify the revocation configuration from the available revocation configurations), and then click Next.4. On the Select CA Certificate Location page, select the location of the CA certificate for which this revocation configuration provides certificate status responses. For the Online Responder to check a certificate's status, the revocation configuration must identify the CA that issued the certificate. The following options are available:Figure 19: Select CA Certificate LocationSelect a certificate for an existing enterprise CA. This option allows selecting the CA certificate from the available CA certificates published in AD DS or by querying a specific CA directly for its certificate. If this option is selected in step 4, the wizard will prompt the user to select the CA certificate by browsing AD DS for published CAs or for CA computer names (Figure 20). After identifying the CA certificate, you can verify the certificate details by clicking the View Selected CA certificate link on the wizard page.Figure 20: Choose CA CertificateSelect a certificate from the local certificate store. This option allows selecting a CA certificate by browsing the certificate store on the current computer. If this option is selected in step 4, the wizard will prompt the user to select the CA certificate by browsing the local certificate store.Import certificate from a file. This option allows selecting a certificate file with a \*.cer extension. If this option is selected in step 4, the wizard will prompt the user to select the CA certificate by browsing the file system for a certificate file with a \*.cer extension.5. On the Select Signing Certificate page (Figure 21), the signing certificate must be specified for each revocation configuration. The following options are available:Automatically select a signing certificate. If this option is selected, the Online Responder will automatically search the Personal certificate store for the computer hosting the Online Responder for a certificate that meets the following conditions: The certificate has an OCSP Signing EKU. The certificate was issued by the CA that was selected in step 4. The certificate is valid. The certificate has a matching private key.If more than one signing certificate is available, then the one with the shortest validity period is selected.The Auto-Enroll for an OCSP signing certificate check box allows configuring the Online Responder to automatically enroll and renew OCSP Response Signing certificates for the specified revocation configuration. If the CA that was selected in step 4 is configured to issue the OCSP Response Signing template, this check box will be selected and the Certification Authority and Certificate Template boxes will be filled in automatically. Otherwise, the Auto-Enroll for an OCSP signing certificate check box will not be selected.Note When the Online Responder's autoenrollment functionality is enabled, the enrolled certificates will be stored in the certificate store for the Online Responder service and not in the certificate store of the local computer. You can view the current configuration signing certificate by using the following procedure.To view the current configuration signing certificate, use the following steps:a. Open the Certificates snap-in.b. Click Service account, and click Next.c. Click Local computer, and click Next.d. Select the Online Responder service from the available services list, and click Finish.e. The signing certificate for the current configuration can be found at the store named: OCSPSVC\<configuration name>.Manually select a signing certificate. If this option is selected, the Online Responder will not assign a signing certificate for the revocation configuration. After the wizard has finished and the revocation configuration is created, it is required to manually select a signing certificate for each of the Online Responder Array members. Until this operation is accomplished, the revocation configuration will not be operational.Use the CA certificate for the revocation configuration. If this option is selected, the Online Responder will use the CA certificate that was selected in step 4 as the signing certificate. This option is available only if the Online Responder is installed on the CA computer.Figure 21: Select Signing Certificate6. After selecting the signing certificate, click Next.7. On the Revocation Provider page, click Provider. Additional information is required to configure the revocation provider. The Revocation Provider Properties dialog box allows configuring the revocation provider by selecting the CRLs and the delta CRLs for the revocation configuration. The Online Responder will use this information to retrieve and cache the CRLs and delta CRLs that will be used to provide certificate status responses. In some cases, the locations of the CRLs will be populated based on information in AD DS. By default, the revocation provider will retrieve a new CRL and delta CRL based on the validity period specified in the CRL. The refresh interval can be manually set by entering a specific refresh interval rate. The minimum interval is five minutes.If the CA is configured to issue delta CRLs, the revocation provider will use the URL provided in the Base CRLs list to retrieve the base CRL and will use the information included in the base CRL itself to retrieve the delta CRLs. The Delta CRLs list should be used only if you would like the revocation provider to retrieve the delta CRLs from a different location than the one specified in the base CRL.Figure 22: Revocation Provider Properties8. To close the Revocation Provider Properties dialog box, click OK.9. To create the revocation configuration, click Finish. |

Note

The revocation provider will always look for a valid CRL and a delta CRL on the local computer before trying to retrieve them from the network. If the Online Responder is installed on the same computer as the CA, the values configured in the revocation provider are ignored.

##### Modifying a revocation configuration

After a revocation configuration is created, it can be modified. This is done by selecting the revocation configuration to be edited from the Revocation Configurations view, and then clicking Edit Properties on the Action menu or in the Actions pane.

Local CRL. The Local CRL tab allows locally managing revoked certificates for a revocation configuration. When this option is used, the Online Responder manages a local list of revoked certificates in addition to the CA CRL and delta CRL. This feature is useful when the CA is not responding and cannot publish CRLs or when the Online Responder cannot retrieve the CRL. The local revocation information supersedes information in a CA-published CRL. For example, if a certificate is listed as revoked in the local CRL but is not listed in the CA-published CRL, the Online Responder will still issue a response in which the specified certificate is revoked.

To add a certificate to the Local revoked certificates list, you first need to select the Enable local CRL check box and then click Add. The Revoked Certificate Details dialog box (Figure 23) requires the certificate's serial number, the revocation reason, and the effective date for the revocation.

Figure 23: Revoked Certificate Details dialog box



Revocation Provider. The Revocation Provider tab allows reconfiguring the revocation provider for the specified revocation configuration. Clicking the Provider button will display the same dialog box as in the Creating Revocation Configuration wizard.

Signing. The Signing tab (Figure 24) allows configuring the following response signing options:

 Hash algorithm. The hash algorithm to be used when signing the response.

 Do not prompt for credentials for cryptographic operations. If the signing key is strongly protected by an additional password, selecting this option means the Online Responder will not prompt the user for the password and will fail silently. Understanding this option is important when using HSMs to store the OCSP signing key. If using an HSM and this option is selected, CryptoAPI is instructed not to show the PIN dialog box for accessing the private key, and the signing operation will fail. If this option is not selected, the PIN dialog box will be displayed the first time the configuration is loaded, which can occur when the service starts or when the revocation configuration is loaded for the first time.

Note

Do not select this option if HSM is used to protect private keys.

 Automatically use renewed signing certificates. This option instructs the Online Responder to automatically use renewed signing certificates without asking the Online Responder administrator to manually assign them.

 Allow Nonce requests. This option instructs the Online Responder to inspect and process an OCSP request nonce extension. If a nonce extension is included in the OCSP request and this option is selected, the Online Responder will ignore any cached OCSP response and will create a new response that includes the nonce provided in the request. If this option is disabled and a request that includes a nonce extension is received, the Online Responder will reject the request with an "unauthorized" error.

Note

The Microsoft OCSP client does not support the nonce extension.

Notes

 If a non-critical extension is included in the request, the Online Responder ignores the extension and provides a response. If a critical extension is included in the request the Online Responder will reject the request with an "unauthorized" error.

 Use any valid OCSP signing certificate. By default the Online Responder will only use signing certificates that are issued by the same CA that issued that certificate being validated. This option allows modifying the default behavior and instructs the Online Responder to use any valid existing certificate that includes the OCSP Signing EKU extension.

Note

Windows Vista does not support this deployment model and will fail if this option is selected.

 Online Responder Identifiers. This option is used to select whether to include the key hash or the subject of the signing certificate in the response. This is required per RFC 2560.

Figure 24: Revocation Configuration dialog box, Signing tab



#### Managing Array members

To manage global settings and revocation configurations on multiple Online Responder computers, the concept of "Array" is introduced. An Array is defined as one or more computers that have the Online Responder service installed, logically grouped and managed by the Online Responder snap-in. All computers that are members of an Array will have the same global settings and the same revocation configurations. For each Array, one member is defined as the Array controller; the role of the Array controller is to help resolve synchronization conflicts and to apply updated revocation configuration information to all Array members.

When you first open the Online Responder snap-in, you will see that one Array member already exists in the console tree. This member is the Array controller, which is the local computer by default.

##### Adding Array members

To add Array members

|  |
| --- |
| 1. In the console tree, click Array Configuration.2. On the Action menu or in the Actions pane, click Add Array Member.3. In the Select Computer dialog box, browse for the Online Responder computer to be added to the Array or type the computer's distinguished name, and then click OK. |

After the new Online Responder is added to the Array, the Online Responder snap-in will automatically synchronize global settings as well as existing revocation configurations.

##### Monitoring and managing Array members

Each member of the Array can be monitored and managed independently. Clicking on a specific Array member node displays the Array member view, which includes revocation configuration status information for each of the revocation configurations as well as some configuration options.

To better identify the status of Array members, the following status codes will be displayed in the console tree:

 Array controller–status okay

 Array controller–status critical

 Array controller–status unknown

 Array controller–status warning

 Array member–status okay

 Array member–status critical

 Array member–status unknown

 Array member–status warning

Manually assigning a signing certificate can be accomplished by using the member view.

To manually assign a signing certificate

|  |
| --- |
| 1. Select an Array member node.2. Select the revocation configuration to assign a signing certificate to.3. On the Action menu or in the Actions pane, click Assign Signing Certificate.4. Select a signing certificate from the available signing certificates list, and then click OK. |

Note

The Assign Signing Certificate operation should be used only when Manually select a signing certificate was selected during the creation of a revocation configuration.

## Enabling Remote Management

The Online Responder can be managed from another computer on which the Online Responder snap-in is installed. To enable remote management, firewall rules need to be configured.

To enable remote management

|  |
| --- |
| 1. Open the Windows Firewall with Advanced Security snap-in.2. Click Inbound Rules.3. In the details pane, right-click Online Responder Service (DCOM-In), and click Enable Rule.4. In the details pane, right-click Online Responder Service (RPC-In), and click Enable Rule.5. Close the Windows Firewall with Advanced Security snap-in. |

## Planning for CA Certificate Renewal

As specified in the "Creating Revocation Configurations" section in this document, a revocation configuration is bound to a specific CA key pair. Therefore, renewing a CA affects the Online Responder's configuration and ongoing maintenance.

When a revocation configuration is created, the CA's certificate key ID is stored as the revocation configuration identifier and used to identify the revocation configuration that should be used to service incoming OCSP requests.

### Understanding Revocation Configuration and CA Certificate Relationship

When a CA certificate is renewed by using the same key pair, an existing revocation configuration that was created for the specified CA will still be valid and no additional configuration is required. When a CA is renewed by using a new key pair, the existing revocation configuration will continue to be valid for the renewed key pair but a new revocation configuration will have to be created for the new CA key pair. Currently there is no automatic way to duplicate existing revocation configuration, and the Online Responder administrator has to manually create such revocation configuration.

### Creating Revocation Configuration for Renewed CA

 In some scenarios, it may be required to create a revocation configuration for an old, but still valid, CA certificate and key pair. In that case, the CA certificate will have to be selected from the local machine store or manually exported from the CA as a \*.cer file and then selected during the Revocation Configuration creation wizard.

## Performing Online Responder Backup and Restore

Backing up the Online Responder revocation configuration and the signing keys is essential for proper operation of the Online Responder.

 Revocation configuration. Although revocation configurations can be re-created, it is recommended that the Online Responder is backed up whenever the revocation configuration changes.

 Signing keys. Since signing keys can be reissued in case of corruption or another disaster, they should be backed up only if the issuing CA key is not available. Because of the limitations described in "Renewing OCSP Response Signing certificates," when using a Windows Server 2003, Enterprise Edition–based CA, OCSP signing keys that are issued to Online Responders should be backed up.

Since Online Responder administration tools can synchronize revocation configurations from the Array controller to the Array members, the backup operation needs to be run only on the Online Responder Array controller, which holds the most up-to-date revocation configuration information. To back up the Online Responder revocation configuration, you should perform a full system state backup.

To extract only the revocation configurations

|  |
| --- |
| 1. Switch to the Array controller computer.2. Open the Registry Editor (regedit.exe).3. Navigate to the following registry hive:HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\OCSPSvc\Responder4. Right-click the hive, and click Export.5. Save the information to a \*.reg file, and store the file for backup. |

As described in "Renewing OCSP Response Signing certificates," backing up OCSP signing keys is required only when using the Online Responder with a Windows Server 2003–based CA. Since OCSP signing keys are unique to each revocation configuration of each Online Responder computer, all signing keys available need to be backed up for each Online Responder computer.

To back up the Online Responder signing keys, you should perform a full system state backup.

## Performing Online Responder Migration

In some scenarios, it may be required to migrate an existing Online Responder Array member to a new computer. As discussed in the "Performing Backup and Restore" section, because Online Responder administration tools can synchronize revocation configurations from the Array controller to the Array members automatically, computer migration is simplified.

To migrate an existing Online Responder Array member to a new computer

|  |
| --- |
| 1. If autoenrollment is not enabled for the Array member being migrated, back up the OCSP signing keys by using the Certificates snap-in.2. To maintain the same name for the migrated Array member, perform the following steps:a. Using the Online Responder snap-in, remove the Array member from the Array.b. In System Properties, delete the Array member from the domain.3. Install the new Array member and join the computer to the domain.4. If required, import previously backed-up signing keys to the computer's machine store by using the Certificates snap-in.5. Using the Online Responder snap-in, add a new Array member and select the new computer. |

## Troubleshooting the Online Responder

Online Responder troubleshooting can be divided into two subcategories.

 Online Responder service–related issues. Problems in this category include request/response issues and revocation provider configuration.

 Online Responder tools–related issues. Problems in this category include all Online Responder snap-in and revocation configuration synchronization–related issues.

### Online Responder Service Problems

Note

For troubleshooting scenarios in which there are no event log errors or warnings and the Online Responder snap-in reports no problems, check the Online Responder service log for further diagnostic information. The service log is located at: SystemDrive\Windows\ServiceProfiles\networkservice\ocspsvc.log

The following events relate to the Online Responder service (ocspsvc.exe) status and are displayed in the computer's Event Viewer.

Event 0xC25A0014 - The Online Responder Service did not start: %1. (Error Message).

Event ID 20

Event Name MSG\_E\_GENERIC\_STARTUP\_FAILURE

Event Source OnlineResponder or OCSPSvc

Description The Online Responder service (ocspsvc.exe) did not start. In most cases, the reason will be included in the event message instead of the argument %1.

Diagnostics The following reasons might cause the service to fail initializing:

 Corrupted registry information

 No system resources

Resolve

1. If the information in the error description does not provide enough information to resolve the error, first try to restart the Online Responder service from the Services snap-in (services.msc). If the Online Responder service fails to start, check the event log for other errors that may be related to this failure.

2. If the registry information is corrupted, you must uninstall and reinstall the Online Responder service by using Server Manager.

3. If not enough system resources are available to start the Online Responder Service, try to restart the computer or free system resources.

Event 0xC25A0015 - %1(FileIdentifier): OCSP Responder Services detected an exception at address %2. Flags = %3. The exception is %4(ErrorCode).

Event ID 21

Event Name MSG\_E\_EXCEPTION

Event Source OnlineResponder or OCSPSvc

Description This event indicates an internal problem with the Online Responder service. Call Microsoft Customer Service and Support to report the issue.

Diagnostics N/A

Resolve N/A

Event 0xC25A0016 - The Online Responder Service did not process a request from %1. The request was very long, which can be caused by a denial-of-service attack. If the request was rejected in error, modify the MaxIncomingMessageSize property for the service. Unless verbose logging is enabled, this error will not be logged again for 20 minutes.

Event ID 22

Event Name MSG\_E\_POSSIBLE\_DENIAL\_OF\_SERVICE\_ATTACK

Event Source OnlineResponder or OCSPSvc

Description N/A

Diagnostics N/A

Resolve It is recommended that the originator of the request is located as this type of event might point to a malicious user or application trying to compromise the Online Responder.

The MaxIncomingMessageSize value can be modified by creating a new registry DWORD value under the HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\OCSPSvc\Responder registry hive and setting the value to the maximum number of bytes you would like the Online Responder to be able to process.

Event 0xC25A0017 - The Online Responder Service could not locate a signing certificate for configuration %1(CAConfigurationID).(%2) (Error Message).

Event ID 23

Event Name MSG\_E\_CACONFIG\_MISSING\_SIGNINGCERT

Event Source OnlineResponder or OCSPSvc

Description This event occurs when the Online Responder service encounters a problem either locating or loading a specific configuration's signing certificate.

Diagnostics The following reasons might cause this event:

 The OCSP Response Signing certificate is not present in the Personal certificate store for the computer.

For AutoEnroll configurations in which the Online Responder service itself enrolls for its certificate, this means that there may have been a problem with enrolling or installing the signing certificate. Check the event log for additional errors or warnings that may be related to this error. Then, check the status of the OCSP Response Signing certificate.

Note

If the revocation configuration is set up for automatic enrollment and renewal of the OCSP Response Signing certificate, the signing certificate is located within the Online Responder service account's certificate store. To view it, open MMC and add the Certificates snap-in for "Service account" on the Online Responder computer, selecting the "Online Responder Service" account. The certificate will be in the certificate store under the node labeled with the revocation configuration name.

If the revocation configuration is set up for manual enrollment and renewal of the OCSP Response Signing certificate, locate the signing certificate within the Online Responder computer's Personal certificate store for the local computer. Open the Certificates snap-in for the computer and locate the signing certificate in the Personal certificate store.

 The OCSP signing certificate private key is not accessible to the Network Service account. To determine if this is the case, see "Enrolling for an OCSP Response Signing Certificate" in the [Configuring the OCSP Response Signing certificate template](#DSDOC_BKMK_ConfiguringtheOCSPResponseSig) section.

 The OCSP Response Signing certificate is not valid for signature purposes. Note that a valid OCSP Response Signing certificate will have "OCSP Signing (1.3.6.1.5.5.7.3.9)" in the EKU extension.

Resolve

1. If an OCSP Response Signing certificate is not present in the Personal certificate store for the local computer, and the revocation is configured for manual OCSP Response Signing certificate enrollment, you should enroll for a certificate manually.

2. For configurations in which the Online Responder service itself enrolls for its certificate, manual enrollment will not work and you should check the event log for additional errors or warnings related to a failure to enroll or install the OCSP Response Signing certificate. If no additional information is available, verify the following:

a. Verify that the computer on which the Online Responder service is running has connectivity to a CA. Use the Certification Authority snap-in on the CA to verify that the CA is configured to issue certificates based on the OCSP Response Signing template.

b. Use the Certificate Templates snap-in to verify that the computer running the Online Responder has Read and Enroll permissions on the OCSP Response Signing template.

3. If a valid OCSP Response Signing certificate exists, ensure that the Online Responder service has access to the private key. By default, the Online Responder service runs as Network Service, so the private key must be accessible by this user context. If the OCSP Response Signing certificate private key is not accessible to Network Service, follow the steps in "Enrolling for an OCSP Response Signing certificate" in the [Configuring the OCSP Response Signing certificate template](#DSDOC_BKMK_ConfiguringtheOCSPResponseSig) section to correct the problem.

4. If the OCSP Response Signing certificate is not valid for signature purposes, ensure that you enroll for a certificate that includes the id-kp-OCSPSigning EKU, labeled "OCSP Signing (1.3.6.1.5.5.7.3.9)."

Event 0x825A0019 - The signing certificate for Online Responder configuration %1 will expire soon.

Event ID 25

Event Name MSG\_W\_CACONFIG\_SIGNINGCERT\_EXPIRING

Event Source OnlineResponder or OCSPSvc

Description The signing certificate for the specified configuration is about to expire. Specifically, if the Online Responder has been configured so that it can automatically enroll for signing certificates, the certificate has entered the period in which it can be automatically re-enrolled. For manual configurations, this means that the period when renewal reminders are triggered has begun.

Diagnostics Review the expiration date of the specified certificate.

Locate the signing certificate as specified in the guidance for Online Responder event 23 above, and note the Valid to field.

If the revocation configuration is set up for automatic enrollment of the OCSP Response Signing certificate, further action may not be required. Check the expiration date on the certificate to ensure you will have adequate time to verify when automatic re-enrollment has occurred.

Resolve For manual configurations, renew the signing certificate. To do this, right-click the certificate, and click Renew Certificate with New Key to start the Certificate Renewal Wizard.

Note

The reminder duration is a responder-wide property, expressed as a percentage of the certificate lifetime. The default value is 90 percent, but this value can be modified by adding a DWORD registry key named ReminderDuration under HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\OcspSvc\Responder\%Revocation Configuration Name\

Enter a value between 1 and 100 to indicate the desired percentage. You must stop and restart the Online Responder service in order for the new value to take effect.

Event 0xC25A001A - The signing certificate for Online Responder configuration %1 has expired. OCSP requests for this configuration will be rejected.

Event ID 26

Event Name MSG\_E\_CACONFIG\_SIGNINGCERT\_EXPIRED

Event Source OnlineResponder or OCSPSvc

Description The signing certificate for the specified configuration has expired.

Diagnostics Review the expiration date of the specified certificate.

 If the revocation configuration is set up for automatic enrollment of the OCSP Response Signing certificate, there may have been a problem with the automatic re-enrollment. Locate the signing certificate within the Online Responder service account's certificate store as specified in the guidance for Online Responder event 23 above. If the certificate has expired, check the event log for additional errors or warnings related to a failure to enroll or to install the OCSP Response Signing certificate automatically. If no other information is available, verify the following:

a. Verify that the computer on which the Online Responder service is running has connectivity to a CA.

b. Use the Certification Authority snap-in on the CA to verify that the CA is configured to issue certificates based on the OCSP Response Signing template or a duplicate of that template.

c. Use the Certificate Templates snap-in to verify that the computer running the Online Responder has Read and Enroll permissions on the OCSP Response Signing template.

 If the revocation configuration is set up for manual enrollment of the OCSP Response Signing certificate, locate the signing certificate within the Online Responder computer's local computer Personal certificate store, as specified in the guidance for Online Responder event 23 above.

Resolve

If the revocation configuration is configured for manual enrollment of the OCSP signing certificate, and a valid, renewed OCSP signing certificate exists on the Online Responder computer, assign the certificate to the revocation configuration identified in the event log by using the following steps:

1. In the Online Responder snap-in, click Array Configuration and click the node for the computer on which the warning was logged.

2. Right-click the revocation configuration identified in the event log, and click Assign Signing Certificate.

3. Select the certificate, and click OK.

4. Click Revocation Configuration, right-click the revocation configuration, and click Edit Properties. Click the Signing tab.

If Automatically use renewed signing certificates is not selected, you will have to reassign the signing certificate to the revocation configuration manually each time the signing certificate is renewed. If you select this option, the assignment will happen automatically.

If there is not a valid, renewed OCSP signing certificate in the local computer personal certificates store on the computer that logged the warning, enroll for a new signing certificate by using the following steps:

1. Right-click the local computer personal certificates store, point to All Tasks, and click Request New Certificate to start the Certificate Enrollment Wizard.

2. Enroll for a certificate based on the OCSP Response Signing template, or a duplicate of that template.

Note

A valid OCSP signing certificate will have "OCSP Signing (1.3.6.1.5.5.7.3.9)" in the Enhanced Key Usage (EKU) extension.

3. Use the steps 1 through 4 in the previous procedure to assign the new certificate to the revocation configuration.

Event 0x825A001B - The signing certificate for Online Responder configuration %1 was not updated.(%2) (Error Message).

Event ID 27

Event Name MSG\_W\_CACONFIG\_UPDATE\_THREAD\_FAILED

Event Source OnlineResponder or OCSPSvc

Description This event can occur if the Online Responder service cannot update the signing certificate in case of renewal.

Diagnostics This should happen only in the case of the system running out of resources.

Resolve If not enough system resources are available for the Online Responder to operate normally, first restart the Online Responder service and then restart the computer or free system resources. If the error persists, call Microsoft Customer Service and Support.

Event 0xC25A001D - Settings for Online Responder configuration %1 cannot be loaded. OCSP requests for this configuration will be rejected (%2) (Error Message).

Event ID 29

Event Name MSG\_E\_CACONFIG\_FAILTOLOAD

Event Source OnlineResponder or OCSPSvc

Description This event can occur if a revocation configuration is corrupted and cannot be loaded.

Diagnostics N/A

Resolve Follow these steps to resolve the problem:

1. Try to delete the revocation configuration through the Online Responder snap-in.

2. Re-create the specified revocation configuration.

If the configuration cannot be loaded through the Online Responder snap-in, follow these steps:

1. Navigate to the following registry hive: HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\OCSPSvc\Responder

2. Locate and delete the corrupted revocation configuration.

Note

If you are encountering this problem on an Array member, you should delete the corrupted configuration from the Array member and then synchronize the Array to re-create the revocation configuration. If you are encountering this problem on an Array controller, temporarily set another computer as the Array controller, synchronize the Array, and then reset the original computer to be the Array controller.

Event 0x825A001F - Performance counters for the Online Responder Service cannot be initialized.

Event ID 31

Event Name MSG\_W\_PERF\_COUNTER\_INIT\_ERROR

Event Source OnlineResponder or OCSPSvc

Description This event indicates an internal problem with the Online Responder service.

Diagnostics The computer hosting the Online Responder may be running low on memory.

Resolve Open a Windows Performance console window (Perfmon.msc) on the Online Responder computer to evaluate system memory usage. If necessary, resolve resource issues by adding physical or virtual memory, or adjusting memory allocation and hard disk use.

Use the Services snap-in to stop and restart the Online Responder service.

If the error persists, call Microsoft Customer Service and Support to report the issue.

Event The Online Responder Service failed to create an enrollment request for the signing certificate template %2 for configuration %1 (%3) (Error Message).

Event ID 33

Event Name MSG\_E\_CACONFIG\_CREATE\_ENROLLMENT\_REQUEST\_FAILED

Event Source OnlineResponder or OCSPSvc

Description The Online Responder service tried to enroll or re-enroll for a signing certificate and encountered an error while generating the certificate request. The error occurred before the request could be submitted to a CA.

Diagnostics Check the event for the names of the certificate template for which the enrollment request was attempted, as well as the error message. Check for other errors either before or after this event in the event log that may provide more information.

Resolve Resolution will depend upon the error message and any other errors or warnings logged.

Event The Online Responder Service encountered an error while submitting the enrollment request for configuration %1 to certification authority %2. The request ID is %3 (%4) (Error Message).

Event ID 34

Event Name MSG\_E\_CACONFIG\_SUBMIT\_ENROLLMENT\_REQUEST\_FAILED

Event Source OnlineResponder or OCSPSvc

Description The Online Responder service tried to enroll or re-enroll for a signing certificate and encountered an error while submitting the certificate request to the CA.

Diagnostics The event description should contain more information about the cause of the error, including the error message and the failed CA request ID, if one was returned.

Verify that the computer on which the Online Responder service is running has connectivity to a CA. Use the Certification Authority snap-in on the CA to verify that the CA is configured to issue certificates based on the OCSP Response Signing template.

Use the Certificate Templates snap-in to verify that the computer running the Online Responder has Read and Enroll permissions on the OCSP Response Signing template.

In addition, the request ID provided as part of the error message can be used on the CA computer to further diagnose the cause of the error.

Resolve After any permissions errors or other errors have been resolved, start a new enrollment by using the Services snap-in to restart the Online Responder service on each Array member, or alternatively by right-clicking Array Configuration in the Online Responder snap-in and clicking Refresh Revocation Data.

If the error persists, check the event log on the CA for any other events related to enrollment failures. Resolve any issues related to processing requests for OCSP Response Signing certificates, and then restart the Online Responder service to reattempt the request.

Event The Online Responder Service failed to install the enrollment response for configuration %1 for the signing certificate template %2. The request ID is %3 (%4) (Error Message).

Event ID 35

Event Name MSG\_E\_CACONFIG\_INSTALL\_ENROLLMENT\_RESPONSE\_FAILED

Event Source OnlineResponder or OCSPSvc

Description The Online Responder service was able to submit an enrollment request for a signing certificate to a CA, but an error occurred while the response to the request was being processed.

Diagnostics Check the event description to verify the name of the revocation configuration, the certificate template for which the enrollment request was attempted, the request ID of the request on the CA, and the error message.

Use the Certification Authority snap-in to check the status and disposition of the certificate request.

If the certificate was issued, ensure that it was signed by the CA certificate associated with the revocation configuration.

Resolve

If the certificate was issued, ensure that it was signed by the CA key associated with the revocation configuration using the following steps:

1. In the Certification Authority snap-in, identify the CA certificate that signed the issued certificate for the request identified in the error message.

2. In the Online Responder snap-in, click Revocation Configuration, right-click the revocation configuration, and click View CA Certificate.

3. If the two certificates do not match, it is possible that the CA certificate has been renewed and that the revocation configuration is configured for the old CA certificate. In order to enable the Online Responder service to request certificates signed by the older (but still valid) CA certificate, open a command line on the CA and enter the following command:

certutil –setreg ca\UseDefinedCACertInRequest 1

4. Restart the CA.

Once you have enabled the CA to issue OCSP signing certificates based on the CA certificate identified in the request, submit a new request and refresh revocation configuration data by using the following steps:

1. In the Online Responder snap-in, right-click Array Configuration, and click Refresh Revocation Data.

2. Ensure that no further errors are reported.

3. Click the Online Responder node, and ensure that the revocation configuration is listed as Working.

Event 0xC25A0011 - The Online Responder web proxy failed to Initialize. %1 (Error Message).

Event ID 17

Event Name MSG\_E\_FAILED\_TO\_INITIALIZE

Event Source OnlineResponderWebProxy or OCSPISAPIExtension

Description The ISAPI extension failed to initialize because of an internal error.

Diagnostics The following reasons might cause the ISAPI extension to fail to initialize:

 The Online Responder service (ocspsvc.exe) is stopped.

 The DCOM security configuration for the IOCSPAdmin interface is incorrect, causing the ISAPI to fail updating Web proxy information.

 Online Responder–wide configuration properties may be corrupt.

Resolve Follow these steps to resolve the problem.

1. Ensure that the ocspsvc.exe service is running.

2. Using the Dcomcnfg command-line tool, ensure that the Network Service has Activate permissions for the IOCSPAdmin interface.

3. If you suspect the Online Responder–wide configuration properties are corrupt, uninstall and re-install the Online Responder service, or follow the guidance for Online Responder event 29 above to delete and refresh the configuration via the registry or synchronization with other Array members.

Event 0x425A0014 - Online Responder Service detected an invalid configuration for the %1 property. The value was changed from %2(ExistingValue) to %3 (AdjustedValue).

Event ID 20

Event Name MSG\_I\_ADJUST\_PROPERTY\_VALUES

Event Source OnlineResponderWebProxy or OCSPISAPIExtension

Description This event indicates that configuration values are not in the permitted range. This can occur if the registry was manually modified.

Diagnostics N/A

Resolve Follow these steps to resolve the problem:

1. For Array members, either synchronize with the Array controller or reinstall the Online Responder service.

2. For Array controllers, temporarily set another member as the Array controller, synchronize the configuration, and then reset the original member as the Array controller. Otherwise, reinstall the Online Responder service.

Event 0xC25D0010 - For configuration %1, Online Responder revocation provider failed to update the CRL Information: %2. (Error Message).

Event ID 16

Event Name MSG\_E\_CRL\_RETRIEVAL\_FAILED

Event Source OnlineResponderRevocationProvider or OCSPRevInfoProvider

Description The Online Responder service could not retrieve a CRL required for the specified revocation configuration.

Diagnostics Follow these steps to diagnose the problem:

1. Use the Online Responder snap-in to verify that the URLs configured for base and delta CRL distribution points are valid.

a. Open the Online Responder snap-in. In the console tree, select the revocation configuration node. In the details pane, right-click the revocation configuration specified in the event description, and then click Edit Properties. Click the Revocation Provider tab, and then click Provider.

b. Note the URLs configured in the Base CRL URLs and Delta CRL URLs lists. Using network tools, verify that these URLs are accessible by the computer running the Online Responder and that they contain CRL files.

2. Use the Certification Authority snap-in to verify the URLs to which the CA will publish base and delta CRLs.

a. Open the Certification Authority snap-in, right-click the relevant CA, and then click Properties. Click the Extensions tab, and note the URLs entered for the CRL Distribution Point (CDP) extension.

b. Note the URLs for which the Publish CRLs to this location or Publish Delta CRLs to this location check boxes are selected. Verify that these map to the same network locations configured as base and delta CRLs in the Online Responder snap-in.

3. On the computer to which the base CRL is published, examine the Freshest CRL extension for the base CRL. Verify that this identifies a location where the delta CRL can be found.

a. Republish the current CRL, if necessary, by typing the following command at a command prompt:

certutil -crl

b. Then, verify that Online Responder service can access the CRL. From the Online Responder snap-in, right-click Array Configuration, and click Refresh Revocation Data.

4. If the error persists, enable CryptoAPI 2.0 Diagnostics for more information.

To learn how to enable CryptoAPI 2.0 Diagnostics and understand the CryptoAPI diagnostics information, see [Enabling CryptoAPI 2.0 Diagnostics](#DSDOC_BKMK_EnablingCryptoAPI2Diagnostics).

Resolve Depending on the results from the troubleshooting steps above and enabling CryptoAPI 2.0 Diagnostics, ensure that the CA publishes CRLs correctly and that they are available to the Online Responder service.

Event 0xC25D0011 - For configuration %1, Online Responder revocation provider either has no CRL information or has stale CRL information.

Event ID 17

Event Name MSG\_E\_INVALID\_CRL

Event Source OnlineResponderRevocationProvider or OCSPRevInfoProvider

Description The Online Responder service could not retrieve a CRL required for the specified revocation configuration.

Diagnostics See diagnostics for event 16 above.

To learn how to enable CryptoAPI 2.0 Diagnostics and understand the CryptoAPI diagnostics information, see [Enabling CryptoAPI 2.0 Diagnostics](#DSDOC_BKMK_EnablingCryptoAPI2Diagnostics).

Resolve Depending on the results from the troubleshooting steps above and enabling CryptoAPI 2.0 Diagnostics, ensure that the CA publishes CRLs correctly and that they are available to the Online Responder service.

Event 0xC25D0012 - For configuration %1, Online Responder revocation provider found a delta CRL referring to a newer Base CRL.

Event ID 18

Event Name MSG\_E\_MISMATCHED\_BASE\_DELTA\_CRL

Event Source OnlineResponderRevocationProvider or OCSPRevInfoProvider

Description This event indicates that the delta CRL and the base CRLs do not match. The Online Responder service downloaded a delta CRL containing updates to a base CRL that cannot be found. A delta CRL cannot be used without a corresponding base CRL; therefore, the delta CRL is not valid.

Diagnostics The following reasons might cause this event:

 The CA has failed to publish the base CRL but published the delta CRL correctly.

 The Online Responder service could not retrieve the base CRL but could retrieve the delta CRL.

Use the following steps to diagnose the problem:

1. Use the Online Responder snap-in to check the URLs for the base and delta CRLs. Follow the steps outlined in event 16 above to make sure the CA and Online Responder URLs are configured correctly for base and delta CRL publishing and retrieval.

2. Use the Certificates snap-in for the Online Revocation service account on the Online Responder computer to locate the current delta CRL. Check the BaseCRLNumber specified in the "delta CRL indicator" extension of the delta CRL. This number should reference the version number of a published base CRL.

3. If this number does not match the version number of a published base CRL, republish both the base and delta CRLs by typing the following command at a command prompt:

certutil –crl

4. Retrieve updated CRL data on the Online Responder. Either restart the Online Responder service on each Array member or right-click Array Configuration in the Online Responder snap-in and click Refresh Revocation Data. Then verify that the base and delta CRLs match.

Note

If the problem persists, you can enable CryptoAPI 2.0 Diagnostics to diagnose the root of the problem. For more information, see [Enabling CryptoAPI 2.0 Diagnostics](#DSDOC_BKMK_EnablingCryptoAPI2Diagnostics).

Resolve Depending on the results from the troubleshooting steps above and enabling CryptoAPI 2.0 Diagnostics, ensure that the CA publishes CRLs correctly and that they are available to the Online Responder service.

### Online Responder Snap-In Messages

#### Array Configuration messages

The following events relate to the status of Array members and are displayed in the Array Configuration view.

Message Offline

Description Offline status of an Array member means that the member could not be contacted to retrieve the Online Responder properties or revocation configuration information.

Diagnose N/A

Resolve Follow these steps to resolve the problem:

1. Ensure that the Array member computer is running.

2. Ensure that the Online Responder service (ocspsvc.exe) is running on the Array member computer.

3. Check network connectivity to the Array member by using the Ping command-line tool.

4. Using the Dcomcnfg command-line tool, validate that the current user has the proper permissions to the IOCSPAdmin interface.

Message Responder Properties not present on Array Controller.

Description This error can occur if Online Responder settings were deleted from the Array controller and the current user does not have the necessary permissions to update the registry.

Diagnose N/A

Resolve A user with permissions to manage the Online Responder should open the Online Responder snap-in. This will allow the synchronization engine to re-synchronize the properties and revocation configurations of the Array.

Message Responder Properties are not synchronized.

Description This message is displayed if an Array member was offline while a revocation configuration or Online Responder properties were changed.

Diagnose N/A

Resolve A user with permissions to manage the Online Responder should open the Online Responder snap-in. This will allow the synchronization engine to re-synchronize the properties and revocation configurations of the Array.

Message Online

Description The Array member is functional.

Diagnose N/A

Resolve N/A

Message Status Unknown

Description Unknown Array member status is displayed if the Array controller is offline and the Array member's properties or revocation configuration information cannot be evaluated. Note that it does not necessarily mean that the Array member is not functional.

Diagnose N/A

Resolve Follow these steps to resolve the problem:

1. Ensure that the Array controller computer is running.

2. Ensure that the Online Responder service (ocspsvc.exe) is running on the Array controller computer.

3. Check network connectivity to the Array controller by using the Ping command-line tool.

4. Using the Dcomcnfg command-line tool, validate that the current user has the proper permissions to the IOCSPAdmin interface.

Message Array Controller Name on Member is Incorrect.

Description This situation can occur if a new Array controller was assigned to the Array and the security settings to the entire Array were modified while the Array member was offline.

Diagnose Follow this step to diagnose the problem:

 Validate that the current user has permissions to the IOCSPAdmin interface.

Resolve A user with permissions to manage the Online Responder should open the Online Responder snap-in. This will allow the synchronization engine to re-synchronize the properties and revocation configurations of the Array. Right-click Array Configuration, and click Synchronize Members with Array Controller to resynchronize the Online Responder's configuration data to all Array members.

Message Array Member Name(s) on Member is Incorrect.

Description This situation can occur if a new Array member was added to the Array and the security settings to the entire Array were modified while the Array member was offline.

Diagnose Follow this step to diagnose the problem:

 Validate that the current user has permissions to the IOCSPAdmin interface.

Resolve A user with permissions to manage the Online Responder should start the Online Responder snap-in. This will allow the synchronization engine to re-synchronize the properties and revocation configurations of the Array. Use the Synchronize members with array controller action of the Array node to resynchronize the Online Responder's configuration data to all Array members.

#### Revocation Configuration messages

The following events relate to the status of the revocation configuration and are displayed in the Online Responder snap-in under the Revocation Configuration view.

Message Revocation Configuration is not synchronized with Array Controller.

Description This situation can occur if a revocation configuration was changed on the Array controller while the Array member was offline.

Diagnose N/A

Resolve Synchronize the Array by using the Online Responder snap-in.

Message Revocation Configuration is missing on Array Controller.

Description This situation can occur if the Online Responder snap-in is targeted at an Array member while the Array controller is offline.

Diagnose N/A

Resolve Follow these steps to resolve the problem:

1. Ensure that the Array controller computer is running.

2. Ensure that the Online Responder service (ocspsvc.exe) is running on the Array controller computer.

3. Check network connectivity to the Array controller by using the Ping command-line tool.

4. Using the Dcomcnfg command-line tool, validate that the current user has the proper permissions to the IOCSPAdmin interface.

Message Revocation Configuration is missing on array member(s).

Description This situation can occur if the Online Responder snap-in is targeted at the Array controller while the Array member is offline.

Diagnose Follow these steps to diagnose the problem:

1. Ensure that the Array member computer is running.

2. Ensure that the Online Responder service (ocspsvc.exe) is running on the Array member computer.

3. Check network connectivity to the Array member by using the Ping command-line tool.

4. Using the Dcomcnfg command-line tool, validate that the current user has the proper permissions to the IOCSPAdmin interface.

Resolve If the Array member is online and available, use the Synchronize members with array controller action of the Array node to resynchronize the Online Responder's configuration data to all Array members.

Message Working

Description "Working" status means that the revocation configuration is functioning as expected.

Diagnose N/A

Resolve N/A

Message Bad signing certificate on Array Controller.

Description This message occurs when the Online Responder service encounters a problem either locating or loading a specific configuration's signing certificate.

Diagnose For diagnostics steps, see event 23 above.

Resolve For resolution steps, see event 23 above.

Message Bad signing certificate on member(s).

Description This message occurs when the Online Responder service encounters a problem either locating or loading a specific configuration's signing certificate.

Diagnose For diagnostics steps, see event 23 above.

Resolve For resolution steps, see event 23 above.

Message Signing certificate status is not yet available for the Array Controller.

Description This message indicates that a signing certificate is not available for the specified revocation configuration.

Diagnose This message can appear after creating or renaming a revocation configuration or after changing signing properties.

Resolve Refresh the information in the Online Responder snap-in by clicking Refresh in the Actions pane.

Message Signing certificate status is not yet available for member(s).

Description This message indicates that a signing certificate is not available for the specified revocation configuration or that a signing certificate is available but has not yet been detected by the revocation configuration.

Diagnose This message can appear after creating or renaming a revocation configuration or after changing signing properties.

Resolve Refresh the start page by clicking Refresh in the Actions pane.

Message Revocation provider is not working on the Array Controller.

Description This message indicates that a revocation provider is incorrectly configured on the Array controller.

Diagnose N/A

Resolve Follow these steps to resolve the problem:

1. Open the revocation provider properties for the specified revocation configuration.

2. Validate that all parameters are correct and within the permitted value range.

Message OCSP signing templates could not be retrieved. %(ErrorMessage).

Description This message indicates that the Online Responder service was not able to retrieve a list of certificate templates able to issue OCSP Response Signing certificates. Because of this, the Online Responder service is not able to enroll for a signing certificate.

Diagnose Follow these steps to diagnose the problem:

1. Verify that the computer on which the Online Responder service is running has connectivity to a CA. Use the Certification Authority snap-in on the CA to verify that the CA is configured to issue certificates based on the OCSP Response Signing template.

2. Use the Certificate Templates snap-in to verify that the computer running the Online Responder has Read, Enroll, and Autoenroll permissions on the OCSP Response Signing template.

Resolve Follow these steps to resolve the problem:

1. Configure the CA to issue certificates based on the OCSP Response Signing template.

2. Use the Certificate Templates snap-in to grant the computer running the Online Responder Read, Enroll, and Autoenroll permissions on the OCSP Response Signing template.

## Enabling CryptoAPI 2.0 Diagnostics

CryptoAPI 2.0 Diagnostics is a new feature in Windows Vista and Windows Server 2008 that makes it easier to troubleshoot PKI-related problems. It logs information about certificate chain building and revocation into the Event Viewer in more detail than previous CryptoAPI troubleshooting tools.

CryptoAPI 2.0 Diagnostics logs events that generally correspond to the CryptoAPI 2.0 APIs that are being called. In addition to the parameters and results of these APIs, it also logs details such as all network retrieval attempts, HTTP errors, and proxy events. If you see problems related to CryptoAPI 2.0 in your application, use this feature to reproduce the problem.

You can enable this feature from the Event Viewer or by using command-line scripts.

To enable CryptoAPI 2.0 Diagnostics from the Event Viewer

|  |
| --- |
| 1. To open the Event Viewer, click Start, right-click My Computer, and then click Manage. Event Viewer is in the Computer Management window under System Tools.Note Event Viewer is an MMC snap-in and you need administrative privileges to access it.2. In the Event Viewer, navigate to Application Logs, Microsoft, Windows, and then CryptoAPI 2.0 for the CryptoAPI 2.0 channel.3. Right-click Operational, and then click Log Properties.4. Select the Enable Logging check box. This enables CryptoAPI 2.0 Diagnostics logging.5. To save the log to a file, right-click Operational, and then click Save Log File as. You can save the log file in the .elf format (which can be opened by using the Event Viewer) or in the standard .xml format.6. If data is present in the logs before you reproduce the problem, it is recommended that you clear the logs. This allows only the data relevant to the problem to be collected from the saved logs. To clear the logs, right-click Operational, and then click Clear Log. |

You can also enable logging and save the logs using the wevtutil.exe tool.

To enable CryptoAPI 2.0 Diagnostics by using command-line scripts

|  |
| --- |
| 1. Right-click the command prompt program icon, and click Run as administrator.2. At the command prompt, use the following commands: To enable logging, type:wevtutil.exe sl Microsoft-Windows-CAPI2/Operational /e:true To save the log to a file, type:wevtutil.exe epl Microsoft-Windows-CAPI2/Operational filename.elf To disable logging, type:wevtutil.exe sl Microsoft-Windows-CAPI2/Operational /e:false To clear logs, type:wevtutil.exe cl Microsoft-Windows-CAPI2/Operational |

## Additional Resources

 Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile (<http://go.microsoft.com/fwlink/?LinkID=71066>)

 RFC 2560, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP" (<http://go.microsoft.com/fwlink/?LinkID=71068>)

 The Internet Engineering Task Force (<http://go.microsoft.com/fwlink/?LinkID=121>)

 Windows Server 2008 CA Enhancements ([http://go.microsoft.com/fwlink/?LinkID=83212](http://go.microsoft.com/fwlink/?LinkID=27081))