Knowledge Base

Enterprise CA May Not Publish Certificates from Child Domain or Trusted Domain

PSS ID Number: 219059

Article Last Modified on 11/21/2003

The information in this article applies to:

- Microsoft Windows Server 2003, Datacenter Edition
- Microsoft Windows Server 2003, Enterprise Edition
- Microsoft Windows Server 2003, Standard Edition
- Microsoft Windows Server 2003, 64-Bit Datacenter Edition
- Microsoft Windows Server 2003, 64-Bit Enterprise Edition
- Microsoft Windows Server 2003, Web Edition
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Datacenter Server

This article was previously published under Q219059

SYMPTOMS

You may not be able to issue certificates using an enterprise Certificate Authority (CA) to users in child domains. When you try to do so, the following entry may appear in the event log:
Event ID: 11
Source: Cert Server Enterprise Policy
Application: Warning CA was unable to publish the certificate for the Domain\server. Server is not part of the Cert Publishers group. Privilege violation.

CAUSE

When you install a child domain in an existing domain tree with an enterprise CA already configured, the default permissions on the child domain do not allow the enterprise CA to publish certificates from the child domain.

STATUS

Microsoft has confirmed that this is a problem in the Microsoft products that are listed at the beginning of this article.

MORE INFORMATION

Certificate servers publish certificates to user objects in the directory service. They are allowed to do this because they are in the Cert Publishers group, which has write access to the 'userCertificate' attribute on the user object.

The problem occurs when a certificate server in one domain tries to issue a certificate to a user in another domain.

WORKAROUND

To work around this issue, use one of the following methods:

- Manually add the CA computer to the Cert Publishers group on the child domain. This process cannot be performed during Setup because the child domain may not yet exist when the CA is configured.

  NOTE: This only works in a Windows Server 2003-based environment, not a Windows 2000 environment.
- Use the Delegation Wizard to manually add the root domain's Cert Publisher group to every user object in the child domain.

Keywords: kbprb KB219059
Technology: kbwin2000AdvServ kbwin2000AdvServSearch kbwin2000DataServ kbwin2000DataServSearch kbwin2000Search kbwin2000Serv kbwin2000ServSearch kbWinAdvServSearch kbWinDataServSearch kbWinServ2003Data kbWinServ2003Data64bit kbWinServ2003Data64bitSearch kbWinServ2003DataSearch kbWinServ2003Ent kbWinServ2003Ent64bit kbWinServ2003Ent64bitSearch kbWinServ2003EntSearch kbWinServ2003Search kbWinServ2003St kbWinServ2003Web