Install an IP-HTTPS Certificate

Applies To: Windows Server 2008 R2/2012/2012r2

Important

This topic describes deployment of DirectAccess in Windows Server 2008 R2. For deployment of DirectAccess in Microsoft Forefront Unified Access Gateway (UAG), see the Forefront UAG DirectAccess Deployment Guide (http://go.microsoft.com/fwlink/?LinkId=179989).

The DirectAccess server needs a customized Secure Sockets Layer (SSL) certificate to authenticate Internet Protocol over Secure Hypertext Transfer Protocol (IP-HTTPS)-based DirectAccess connections.

To complete these procedures, you must be a member of the local **Administrators** group, or otherwise be delegated permissions to request and customize an SSL certificate. Review details about using the appropriate accounts and group memberships at Local and Domain Default Groups (http://go.microsoft.com/fwlink/?LinkId=83477).

To obtain an additional certificate for IP-HTTPS

1. On the DirectAccess server, click **Start**, type **mmc**, and then press ENTER. Click **Yes** at the User Account Control prompt.
2. Click **File**, and then click **Add/Remove Snap-ins**.
3. Click **Certificates**, click **Add**, click **Computer account**, click **Next**, select **Local computer**, click **Finish**, and then click **OK**.
4. In the console tree of the Certificates snap-in, open **Certificates (Local Computer)\Personal\Certificates**.
5. Right-click **Certificates**, point to **All Tasks**, and then click **Request New Certificate**.
6. Click **Next** twice.
7. On the **Request Certificates** page, click the Web Server certificate template, and then click **More information is required to enroll for this certificate**.

   If the Web Server certificate template does not appear, ensure that the DirectAccess server computer account has enroll permissions for the Web Server certificate template. For more information, see Configure Permissions on the Web Server Certificate Template.

8. On the **Subject** tab of the **Certificate Properties** dialog box, in **Subject name**, for **Type**, select **Common name**.
9. In **Value**, type the fully qualified domain name (FQDN) of the Internet name of the DirectAccess server (for example, **da1.contoso.com**), and then click **Add**.
10. Click **OK**, click **Enroll**, and then click **Finish**.
11. In the details pane of the Certificates snap-in, verify that a new certificate with the FQDN was enrolled with **Intended Purposes** of **Server Authentication**.

12. Right-click the certificate, and then click **Properties**.
13. In **Friendly Name**, type **IP-HTTPS Certificate**, and then click **OK**.

Note

Steps 12 and 13 are optional, but make it easier for you to select the certificate for Secure Hypertext Transfer Protocol (HTTPS) connections in Step 2 of the DirectAccess Setup Wizard.

⚠**Warning**

The DirectAccess Setup Wizard by default configures the URL of the IP-HTTPS server in the DirectAccess client and server GPOs based on the following format: https://*SubjectFieldIP-HTTPSCertificate*:443://IPHTTPS. This URL must not be more than 256 characters long. Otherwise, the IP-HTTPS component on the DirectAccess client and server will not operate correctly. Therefore, the FQDN in Step 9 of this procedure must not be more than 234 characters.