Set up WinRM in XL Deploy and on a target host

* [Domain accounts](https://docs.xebialabs.com/xl-deploy/how-to/set-up-winrm-in-xl-deploy-and-on-a-target-host.html#domain-accounts)
* [Password limitations](https://docs.xebialabs.com/xl-deploy/how-to/set-up-winrm-in-xl-deploy-and-on-a-target-host.html#password-limitations)
* [For more information](https://docs.xebialabs.com/xl-deploy/how-to/set-up-winrm-in-xl-deploy-and-on-a-target-host.html#for-more-information)

To use the WINRM\_INTERNAL or the WINRM\_NATIVE connection type, set up [Microsoft Windows Remote Management (WinRM)](http://msdn.microsoft.com/en-us/library/aa384426(v=vs.85).aspx) on the remote host:

1. If the remote host is running Windows Server 2003 SP1 or SP2, or Windows XP SP2, install the [WS-Management v.1.1 package](http://support.microsoft.com/default.aspx?scid=kb;EN-US;936059&wa=wsignin1.0).
2. If the remote host is running Windows Server 2003 R2, go to **Control Panel** > **Add/Remove System Components** and add WinRM under **Management and Monitoring Tools**. Then, install the [WS-Management v.1.1 package](http://support.microsoft.com/default.aspx?scid=kb;EN-US;936059&wa=wsignin1.0) to upgrade the WinRM installation.
3. If the remote host is running Windows Vista or Windows 7, the **Windows Remote Management (WS-Management)** service is not started by default. Start the service and change its startup type to **Automatic (Delayed Start)** before proceeding.
4. On the remote host, open a command prompt (not a PowerShell prompt) using the **Run as Administrator** option and paste in the following lines.

When using the WINRM\_INTERNAL connection type:

winrm quickconfig

y

winrm set winrm/config/service/Auth @{Basic="true"}

winrm set winrm/config/service @{AllowUnencrypted="true"}

winrm set winrm/config/winrs @{MaxMemoryPerShellMB="1024"}

winrm set winrm/config/client @{TrustedHosts="\*"}

When using the WINRM\_NATIVE connection type:

winrm quickconfig

y

winrm set winrm/config/service/Auth @{Basic="true"}

winrm set winrm/config/winrs @{MaxMemoryPerShellMB="1024"}

Or keep reading for more detailed instructions.

1. Run the quick config of WinRM to start the Windows Remote Management service, configure an HTTP listener, and create exceptions in the Windows Firewall for the Windows Remote Management service:
2. winrm quickconfig

**Note:** The Windows Firewall must be running to run this command. See [Microsoft Knowledge Base article #2004640](http://support.microsoft.com/kb/2004640).

1. (Optional) By default, basic authentication is disabled in WinRM. Enable it if you are going to use local accounts to access the remote host:
2. winrm set winrm/config/service/Auth @{Basic="true"}
3. (Optional) By default, Kerberos authentication is enabled in WinRM. Disable it if you are **not** going to use domain accounts to access the remote host:
4. winrm set winrm/config/service/Auth @{Kerberos="false"}

**Note:** Do not disable **Negotiate authentication**, as the winrm command itself uses it to configure the WinRM subsystem.

1. (Only required for WINRM\_INTERNAL or when the property winrsUnencrypted is set to true) Configure WinRM to allow unencrypted SOAP messages:
2. winrm set winrm/config/service @{AllowUnencrypted="true"}
3. Configure WinRM to provide enough memory to the commands that you are going to run (that is, 1024 MB):
4. winrm set winrm/config/winrs @{MaxMemoryPerShellMB="1024"}

**Note:** This is not supported by WinRM 3.0, which is included with the Windows Management Framework 3.0. This update [has been temporarily removed from Windows Update](http://blogs.msdn.com/b/powershell/archive/2012/12/20/windows-management-framework-3-0-compatibility-update.aspx) because of numerous incompatibility issues with other Microsoft products. However, if you have already installed WMF 3.0 and cannot downgrade, [Microsoft Knowledge Base article #2842230](http://support.microsoft.com/kb/2842230) describes a hotfix that can be installed to re-enable the MaxMemoryPerShellMB setting.

1. Configure WinRM to accept connections from trusted hosts:
2. winrm set winrm/config/client @{TrustedHosts="\*"}

**Note:** This is not always required and the command as given will accept connections from all hosts. This command can be refined by specifying hostnames. For example:

winrm set winrm/config/client @{TrustedHosts="host1,host2..."}

1. To use the WINRM\_INTERNAL or WINRM\_NATIVE connection type with HTTPS (that is, with winrmEnableHttps set to true), follow these steps:

(Optional) Create a self-signed certificate for the remote host by installing selfssl.exe from [the IIS 6 resource kit](http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=17275) and running the command below or by following the instructions [in this blog post by Hans Olav](http://www.hansolav.net/blog/SelfsignedSSLCertificatesOnIIS7AndCommonNames.aspx):

C:\Program Files\IIS Resources\SelfSSL>selfssl.exe /T /N:cn=HOSTNAME /V:3650

Microsoft (R) SelfSSL Version 1.0

Copyright (C) 2003 Microsoft Corporation. All rights reserved.

Do you want to replace the SSL settings for site 1 (Y/N)?Y

The self signed certificate was successfully assigned to site 1.

Open a PowerShell window and enter the following command to find the thumbprint for the certificate for the remote host:

PS C:\Windows\system32> Get-childItem cert:\LocalMachine\Root\ | Select-String -pattern HOSTNAME

[Subject]

CN=HOSTNAME

[Issuer]

CN=HOSTNAME

[Serial Number]

527E7AF9142D96AD49A10469A264E766

[Not Before]

5/23/2011 10:23:33 AM

[Not After]

5/20/2021 10:23:33 AM

[Thumbprint]

5C36B638BC31F505EF7F693D9A60C01551DD486F

Create an HTTPS WinRM listener for the remote host with the thumbprint you’ve just found:

winrm create winrm/config/Listener?Address=\*+Transport=HTTPS @{Hostname="HOSTNAME"; CertificateThumbprint="THUMBPRINT"}

If you are using the WINRM\_INTERNAL connection type, add the self-signed certificate to the JVM trusted keystore as described in [this blog post](http://blog.nerdability.com/2013/01/tech-how-to-fix-sslpeerunverifiedexcept.html).

For more information about WinRM, refer to [the online documentation at Microsoft’s DevCenter](http://msdn.microsoft.com/en-us/library/windows/desktop/aa384426(v=vs.85).aspx).

Domain accounts

For the WINRM\_INTERNAL connection type, domain accounts must be specified using the new-style domain syntax; that is, USER@FULL.DOMAIN.

For the WINRM\_NATIVE connection type, domain accounts can be specified using either the new-style (USER@FULL.DOMAIN) or old-style (DOMAIN\USER) domain syntax.

For both connection types, local accounts must be specified without an at-sign (@) or a backslash (\).

**Note:** When using domain accounts with the WINRM\_INTERNAL connection type, the Kerberos subsystem of the Java Virtual Machine must be configured correctly. Please refer to [the information on Kerberos](https://docs.xebialabs.com/xl-deploy/how-to/set-up-kerberos-for-a-winrm-connection.html).

Password limitations

Due to a limitation of the winrs command, passwords containing a single quotation mark (') or a double quotation mark (") cannot be used with the WINRM\_NATIVE connection type.

For more information

For more information about WinRM, refer to [Useful WinRM commands](https://docs.xebialabs.com/xl-deploy/how-to/useful-winrm-commands.html).