Requesting Access to IBM Director Agent on Windows

Planning / Implementation (withdrawn product)

Main

When IBM Director Server first discovers a managed system, that system might be initially locked (represented by padlock icon next to the system) and require the appropriate credentials be supplied before being able to be managed.

To manage such locked systems, you must right-click the inaccessible system and select **Request Access**. You then need to specify an account with administrative privileges on the system you are attempting to access. For Linux systems, you can just use the root user ID; however for Windows, the proper credentials vary depending on the type of agent on the remote system.

Tip: You can select multiple systems before requesting access by using Shift-click or Ctrl-click. In this manner, you can request access to all systems using the same credentials in a single operation.

Requesting access to Windows managed systems provides some challenges if domain credentials are supplied. The format of the user name and domain name varies depending on the level of IBM Director Agent installed on the managed system. Refer to Table 1 for acceptable formats for supplying domain credentials to Windows-based systems.

Table 1: Windows domain credentials for accessing secured systems

Director agent level	Domain credential formats accepted
Level-0 (agentless)	username@domain *Blank passwords are not acceptable.*
Level-1 (Core Services)	username@domain domain\username *Blank passwords are not acceptable.*
Level-2 (full agent)	domain\username *Blank passwords are not acceptable.*

Level-0 systems

For Level-0 systems (agentless), the process depends, generally, on the operating system of the target. More accurately, it depends on the protocol used for communication. By default, IBM Director uses DCOM to communicate with all Level-0 Windows systems, while using SSH for all other operating systems on all platforms. You can choose to use SSH on Windows systems as well by installing the Open SSH software included on the IBM Director installation CD (in the coresvcs directory).

During Level-0 system discovery, these systems are discovered and added to the management console in a secure state (padlock icon ). Management of these systems is not possible until access is granted using the Request Access task.

Requesting access to Level-0 Windows systems

Level-0 Windows systems require an account with local administrative privileges to successfully be granted access from the Request Access task. You can specify either a local administrative account or domain administrative account, but you must specify the account in either of the following formats:

- username (local accounts)
- username@domain (domain accounts)

If the user name on a Windows Level-0 secured system is local system account and the same user name exists as a domain account, IBM Director uses the local account for authentication, unless you specify the domain using username@domain. This can cause problems if you have a domain account with the same user name as a local account.

Tip: You cannot use the syntax domain\username to unlock Level-0 systems.

Level-1 systems

For Level-1 systems (IBM Director Core Services), SSL secures all communication. When IBM Director Server is installed, a self-signed security certificate is created. During Level-1 system discovery, these systems are discovered and added to the management console in a secure state (padlock icon). Management of these systems is not possible until access is granted using the Request Access task.

Requesting access to Level-1 Windows systems

Level-1 Windows systems require an account with local administrative privileges to successfully be granted access from the Request Access task. You can specify either a local administrative account or domain administrative account, but you must specify the account in either of the following formats:

- username (local accounts)
- username@domain or domain\username (domain accounts)

Tip: Unlike Level-0 or Level-2, you can use either username@domain or domain\username to unlock Level-1 systems.

Upon acceptance of the proper Request Access credentials, the security certificate is pushed to the CIMOM (WMI for Windows, Pegasus for all other operating systems and platforms) on the managed system. This certificate is used to open a secure pipe between IBM Director Server and the managed system for all subsequent sessions.

Tip: The certmgr command, available in the DIRCLI command line interface to IBM Director Server, can be used to generate, import, distribute, and revoke security certificates for Level-1 managed systems. Note, however, that the certificates created using this command expire after one year. For more information about this and other DIRCLI commands, see Appendix A: IBM Director commands in the *IBM Director Systems Management Guide*, available from:
http://www.ibm.com/systems/management/director/resources

Level-2 systems

For Level-2 systems (IBM Director Agent), the process is a bit more complex, although invisible to the management console user. It works like this:

1. IBM Director Server attempts to access IBM Director Agent. IBM Director Server bids the public keys that correspond to the private keys it holds.
2. IBM Director Agent checks these keys. If it considers the keys to be trusted, IBM Director Agent replies with a challenge that consists of one of the trusted public keys and a random data block.
3. IBM Director Server generates a digital signature of the random data block using the private key that corresponds to the public key included in the challenge. IBM Director Server sends the signature back to IBM Director Agent.
4. IBM Director Agent uses the public key to verify that the signature is a valid signature for the random data block. If the signature is valid, IBM Director Agent grants access to IBM Director Server.

Requesting access to Level-2 Windows systems

Level-2 Windows systems require an account with local administrative privileges to successfully be granted access from the Request Access task. You can specify either a local administrative account or domain administrative account, but you must specify the account in either of the following formats:

- username (local accounts)
- username\domain (domain accounts)

Tip: You cannot use the syntax username@domain to unlock Level-2 systems.

Windows authentication issues

Issues can arise if you have duplicate user names for local users and domain users or supply domain credentials in the incorrect format, which might prevent you from accessing Windows-based managed systems.

Scenario 1

Local administrator account - username: JohnD, password: 1234
Domain administrator account - JohnD, password: 5678

If you request access to the system with the user name JohnD, IBM Director uses the local system account JohnD and authenticates against password 1234. If you specify JohnD with the password 5678, the request fails because the password is incorrect for the local system account. You need to specify the local system account JohnD with the password 1234 or specify the domain account JohnD@domain (Level-0, Level-1) or domain\JohnD (Level-1, Level-2) with the password 5678 to gain access.

Scenario 2

Local user account - username: JohnD, password: 1234
Domain administrator account - JohnD, password: 5678

If you request access to the system with the user name JohnD, IBM Director uses the local system account JohnD and authenticates against password 1234. If you specify JohnD with the password 1234, the request for access fails because the user does not have local administrative privileges. If you specify JohnD with password 5678, the request fails because the password is incorrect for the local system account. You need to specify JohnD@domain (Level-0, Level-1) or domain\JohnD (Level-1, Level-2) with the password 5678 to gain access.

Related product families

Product families related to this document are the following:

- IBM Systems Director

Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service. Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
8001 Development Drive
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION ”AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary. Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk. Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

This document, TIPS0656, was created or updated on February 13, 2007.

Send us your comments in one of the following ways:

- Use the online Contact us review form found at:
  https://lenovopress.lenovo.com/TIPS0656
- Send your comments in an e-mail to:
  comments@lenovopress.com

This document is available online at https://lenovopress.lenovo.com/TIPS0656.

Trademarks

Lenovo and the Lenovo logo are trademarks or registered trademarks of Lenovo in the United States, other countries, or both. A current list of Lenovo trademarks is available on the Web at https://www.lenovo.com/us/en/legal/copytrade/.

The following terms are trademarks of Lenovo in the United States, other countries, or both:
Lenovo®

The following terms are trademarks of other companies:

Linux® is the trademark of Linus Torvalds in the U.S. and other countries.

Microsoft® and Windows® are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.