**Authentication: Local vs. Remote**

**Local authentication** uses the current domain-joined workstation to contact a domain controller (DC) to authenticate a user’s username and password.

**Remote authentication** uses a remote domain-joined server to authenticate a user’s username and password against a DC.

**Limitations for Local Authentication**

- The local authentication configuration does not provide advance password expiration notice, nor does it provide the password policy information (such as password length and complexity rules) when a user is prompted to enter a new password.

- Local authentication will not function for non-domain joined workstations. To perform password validation, the local machine must be able to contact a DC to authenticate the user’s credential.

- Local authentication is performed as an “interactive login”, which allows the users account information to be locally cached (performed automatically by the operating system) which may not be a desired activity.

**Features and Benefits of Remote Authentication**

- Remote authentication is performed on a domain-joined server on behalf of the user. The HCI Remote Authentication Server service can be configured to run as a user with higher permissions than standard users, while still maintaining domain policies for security. This allows the service to communicate directly with a DC to query the necessary user information to provide advanced password complexity and expiration details (including fine grained password expiration settings).

- Remote authentication will perform a high-performance batch login for the user. Batch login is designed to process many logins and is often used for applications such as mail servers or web sites that perform user validation. According to most sources\(^1\), the user credentials used for batch logins will not be cached by the operating system.

- Remote authentication allows programs running on non-Windows workstations to authenticate against a Windows domain. Because the authentication happens on a remote Windows server that is a domain member, the account can be validated on behalf of the user using a non-Windows platform.

\(^1\) See Page 3 for industry references
Security Concerns

Many sources advise network administrators to disable the ability for workstations to be able to perform a batch login, and to not allow for normal domain users to authenticate or perform batch login. One such advisory source is the "CIS Microsoft Windows 7 Benchmark" document from the Center for Internet Security. ([https://benchmarks.cisecurity.org/downloads/show-single/index.cfm?file=windows7.300](https://benchmarks.cisecurity.org/downloads/show-single/index.cfm?file=windows7.300))

HealthCast agrees with this recommendation as it applies to workstations. In the case of HCI Remote Authentication Server service, the document does not apply as Remote Authentication is a server-based technology. As part of the recommendation against Logon as Batch profile, the referenced document specifically states the following:

On system’s running IIS or ASP.NET, the IIS_WPG group and the `IUSR_<ComputerName>, ASPNET, and IWAM_<ComputerName>` accounts require this user right for IIS to function properly.

On server operating systems, the HCI Remote Authentication Server service has the same requirement as IIS and many Mail server packages (such as Exchange), but this should not be confused with any requirement for enabling batch login on endpoint/workstations.

It is interesting to note that the document specifically references Windows 7 which is not typically used to run an Internet Information Server (IIS) (though it can be done). In addition, typical corporate scenarios preclude using client workstations as multiple-user services, as this violates the Microsoft licensing model. In conjunction with that, the HealthCast eXactACCESS server will not allow itself to be installed on client operating systems (Windows 7, 8, 8.1, or 10) and is designed only to function with server operating systems (Windows 2008, Windows 2012, and Windows 2016) where the expected operation is multi-user access.

Perhaps a more relevant document is "CIS Microsoft Windows Server 2012 Benchmark" or "CIS Microsoft Windows Server 2012 R2 Benchmark".

The Log on as a batch job user right presents a low-risk vulnerability. For most organizations, the default settings are sufficient.

This document also scores the Profile Applicability only to Level 1 - Domain Controller, indicating only servers acting as DCs need to be restricted to administrators only. Further, it makes the same reference to the requirements of IIS that the Windows 7 document provides, noting that IIS may not function if these rights are restricted.
**Microsoft reference**


LOGON32_LOGON_BATCH

This logon type is intended for batch servers, where processes may be executing on behalf of a user without their direct intervention. This type is also for higher performance servers that process many plaintext authentication attempts at a time, such as mail or web servers.

The authentication functions provided by the HCI Remote Authentication Server service performs account impersonation before accessing a local file. This ensures the user has not been denied access for login or access to the validation file. This forces the Windows security layer to perform account validation and restriction verification for the user, maintaining the security integrity of the account in the operating system.

As stated in the Microsoft documentation, Log on as Batch functionality is specifically intended for this type of user authentication. It is unclear whether the operating system will cache these credentials or not, and there appears to be no setting to indicate if it should or should not. Those details are under the exclusive control of the operating system implementation. The references below all indicate that Logon user does not cache credentials for this logon type, but there is no confirmation from Microsoft that this is the case for any given implementation of their operating system. Previous versions of MSDN are no longer available to confirm the statements as outlined below. Given the pervasiveness of this statement, we can only conclude that at one point, it was intended for the OS to NOT cache this type of logon, but perhaps Microsoft has changed the implementation to enhance performance for new scenarios in recent releases of Windows.

**Other References:**


LOGON32_LOGON_BATCH

This logon type is intended for batch servers, where processes may be executing on behalf of a user without their direct intervention; or for higher performance servers that process many clear-text authentication attempts at a time, such as mail or web servers. LogonUser does not cache credentials for this logon type.

http://timgolden.me.uk/pywin32-docs/win32security_LOGON32_LOGON_BATCH.html

LOGON32_LOGON_BATCH

const win32security.LOGON32_LOGON_BATCH;

This logon type is intended for batch servers, where processes may be executing on behalf of a user without their direct intervention; or for higher performance servers that process many clear-text authentication attempts at a time, such as mail or web servers. LogonUser does not cache credentials for this logon type.

**.Net Security Blog**

https://blogs.msdn.microsoft.com/shawnfa/2005/03/21/how-to-impersonate/
**BATCH**

<table>
<thead>
<tr>
<th>4</th>
<th>SeBatchLogonRight / SeDenyBatchLogonRight</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Perform a batch logon. This is intended for servers where logon performance is vital. LogonUser will not cache credentials for a user logged in with this type.</td>
</tr>
</tbody>
</table>

**Conclusion**

Given the low security risk of Logon as batch job permissions as outlined previously, and the references that batch logons are intended to be excluded from the cache, we feel that enabling Logon as a batch job for the user the HCI Remote Authentication Server service installed with eXactACCESS® falls within the intended security context as documented by Microsoft, and that it satisfies the security concerns of our clients as outlined in this document.