VMS Software

VSI Kerberos V3.3-5A for VSI OpenVMS

Release Notes

Publication Date: July 2026

Operating Systems: VSI OpenVMS x86-64 V9.2-3 or higher
VSI OpenVMS IA-64 V8.4-2L1 or higher
VSI OpenVMS Alpha V8.4-2L1 or higher

Software Versions: VSI Kerberos V3.3-5A for OpenVMS x86-64
VSI Kerberos V3.3-5A for OpenVMS IA-64
VSI Kerberos V3.3-5A for OpenVMS Alpha

Kit Names: VSI-X86VMS-KERBEROS-V0303-5A-1.PCSI
VSI-I64VMS-KERBEROS-V0303-5A-1.PCSI
VSI-AXPVMS-KERBEROS-V0303-5A-1.PCSI

VMS Software, Inc. (VSI)
Boston, Massachusetts, USA

VSI Kerberos V3.3-5A for VSI OpenVMS Release Notes

Copyright © 2026 VMS Software, Inc. (VSI), Boston, Massachusetts, USA

Legal Notice

Confidential computer software. Valid license from VSI required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for VSI products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. VSI shall not be liable for technical or editorial errors or omissions contained herein.

All other trademarks and registered trademarks mentioned in this document are the property of their respective holders.

Table of Contents

1. Introduction

VMS Software, Inc. (VSI) is pleased to introduce VSI Kerberos V3.3-5A for OpenVMS x86-64, VSI Kerberos V3.3-5A for OpenVMS IA-64, VSI Kerberos V3.3-5A for OpenVMS Alpha (referred to as VSI Kerberos V3.3-5A later on in this document).

Kerberos V3.3-5A for OpenVMS is based on MIT Kerberos V5 Release 1.4.1. The MIT documentation is available at the MIT Kerberos 5 Release 1.4.1 [https://web.mit.edu/Kerberos/krb5-1.4/krb5-1.4.1.html] website.

2. Acknowledgements

VMS Software, Inc. acknowledges the MIT Kerberos Team and the MIT Kerberos Consortium for their ongoing efforts in developing and supporting this open-source software.

3. What is New in This Release

- The template files included in the kit, KDC_CONF.TEMPLATE and KRB5_CONF.TEMPLATE, have been updated.
- The MIT-produced documentation PostScript files found in KRB$ROOT:[DOC] have been replaced with PDF files.

4. Installing the Kit

The Kerberos product can be installed by a suitably privileged user via the following command:

```
$ PRODUCT INSTALL KERBEROS
```

The installation will then proceed as follows (note that, depending on the platform and some other factors, your output may slightly differ from that shown below):

```
Performing product kit validation of signed kits ...

%PCSI-I-VSIVALPASSED, validation of $1$DGA86:[SYSTEM]VSI-x86VMS-KERBEROS-V0303-5A-1.PCSI
$COMPRESSED;1 succeeded

The following product has been selected:
    VSI X86VMS KERBEROS V3.3-5A             Layered Product

Do you want to continue? [YES]

Configuration phase starting ...

You will be asked to choose options, if any, for each selected product and for
any products that may be installed to satisfy software dependency requirements.

Configuring VSI X86VMS KERBEROS V3.3-5A

Do you want the defaults for all options? [YES]

Do you want to review the options? [NO]

Execution phase starting ...

The following product will be installed to destination:
    VSI X86VMS KERBEROS V3.3-5A             DISK$PIPPIN_SYS:[VMS$COMMON.]
The following product will be removed from destination:
    VSI X86VMS KERBEROS V3.3-3              DISK$PIPPIN_SYS:[VMS$COMMON.]

Portion done: 0%...10%...20%...30%...40%...50%...60%...70%...90%...100%

The following product has been installed:
```

```
    VSI X86VMS KERBEROS V3.3-5A             Layered Product
The following product has been removed:
    VSI X86VMS KERBEROS V3.3-3              Layered Product

VSI X86VMS KERBEROS V3.3-5A

    Configure and set up Kerberos

    If Kerberos will be run on this system, but has not been
    used previously, you need to perform the following steps.

     o Run the Kerberos configuration procedure:

        @SYS$STARTUP:KRB$CONFIGURE.COM

     o Add the following line to SYS$MANAGER:SYSTARTUP_VMS.COM:

        $ @SYS$STARTUP:KRB$STARTUP

     o Add the following line to SYS$MANAGER:SYLOGIN.COM:

        $ @SYS$MANAGER:KRB$SYMBOLS
```

5. Windows Domain Integration

The OpenVMS host can be configured to use existing Windows Active Directory Kerberos KDCs (domain controllers). VSI recommends using the SYS$STARTUP$CONFIGURE.COM procedure to initially configure the host with a single Windows Active Directory Kerberos KDC in the default realm.

To configure the Kerberos client, follow these steps:

1. Start the configuration procedure:

   ```
   $ SYS$STARTUP:KRB$CONFIGURE
   ```

2. The following menu is displayed:

   ```
   Kerberos V3.3-5A for OpenVMS Configuration Menu
     Configuration options:
              1  -  Setup Client configuration
              2  -  Edit Client configuration
              3  -  Setup Server configuration
              4  -  Edit Server configuration
              5  -  Shutdown Servers
              6  -  Startup Servers
              E  -  Exit configuration procedure
     Enter Option:
   ```

   Select option **`1 - Setup Client configuration`**.

3. At the `Where will the OpenVMS Kerberos 5 KDC be running` prompt, specify the short hostname of a Windows Active Directory domain controller in the chosen default realm in lowercase and press Enter. Do not specify an IP address and do not specify the fully qualified domain name of the Windows host. For example, if the Windows host with the fully qualified domain name is *adsrv1.company.com*, specify *adsrv1*.

4. At the `What is the OpenVMS Kerberos 5 default domain` prompt, specify the DNS domain name of the Windows host entered at the previous prompt and press Enter. Specify the domain name in lowercase. For example, *company.com*.

5. At the `What is the OpenVMS Kerberos 5 Realm name` prompt, specify the Active Directory realm name and press Enter. The realm name is identical to the Active Directory domain name. For example, *company.com*.

6. When the procedure returns to the main menu, you can:

- Enter **2 - Edit Client configuration** to modify the generated KRB$ROOT:[ETC]KRB5.CONF file, or
- Enter **E** to exit the configuration procedure.

7. After the initial configuration, edit the KRB$ROOT:[ETC]KRB5.CONF file to add secondary KDCs, username mapping rules, explicit username mappings, domain-to-realm mappings, and additional realms.

6. Kerberos ACME Agent Notes

Kerberos for OpenVMS includes a Kerberos ACME agent that supports external authentication. For more information see section 2.9 of the HP Open Source Security for OpenVMS Volume 3: Kerberos [https://docs.vmssoftware.com/docs/HP_Open_Source_Security_Vol3.pdf].

The following considerations and restrictions apply when configuring and using Kerberos for external authentication on OpenVMS:

- Kerberos usernames are limited to 16 characters.
- Kerberos is case-sensitive. Usernames are typically specified in lowercase, and realm names are typically specified in uppercase.
- During login, quotation marks may be required to preserve the case of the Kerberos principal name. If a realm name is specified, enclose the complete principal name in quotation marks when necessary.
- Users in the default realm can log in using only the username and omit the @REALM portion of the Kerberos principal name.
- Users in nondefault realms must specify their full Kerberos principal name (*username*@REALM), when logging in.
- The Kerberos ACME agent supports logins by users from multiple realms and explicit username mapping.
- After modifying KRB5.CONF, restart ACME_SERVER for the changes to take effect.

The following sections illustrate the syntax required when specifying a Kerberos principal name (*username*@REALM) for many common client applications.

OpenSSH for OpenVMS

- SSH client

  Include the Kerberos principal name within double quote characters, followed by @*target-host* or use the lowercase `-l` option. For example:

  ```
  ssh "username@REALM"@target-host
  ssh -l "username@REALM" target-host
  ```

  ### Important

  Note that, in the second example, the target host name is specified as a separate argument and is not preceded by the at sign (@).

- SFTP and SCP clients

  Include the Kerberos principal name within double quote characters, followed by @*target-host*:

  ```
  sftp "username@REALM"@target-host
  ```

  Note

  OpenSSH for OpenVMS client utilities do not support the URI format when connecting to a target host, such as `ssh://user@host`.

TCP/IP Services for OpenVMS

- SSH client

  Use the lowercase `-l` option to specify the Kerberos principal name within double quote characters. For example:

  ```
  ssh -l "username@REALM" host
  ```

- SFTP and SCP clients

  Do not accept a Kerberos principal name.

OpenSSH for Windows

SSH, SFTP, and SCP clients require the Kerberos principal name to be specified as the username. Quotation marks are not required. For example:

```
ssh username@REALM@host
```

Specify a URI which includes the Kerberos principal name. The URI format is:

```
service://username@REALM@host
```

where *service* is the utility being used (SSH, SFTP, or SCP).

The following examples connect to host `vmsnode1.mycompany.com` using the Kerberos principal name `user1@OTHER.REALM`:

- **Example 1. SSH**

  ```
  ssh ssh://user1@OTHER.REALM@vmsnode1.mycompany.com
  ```

- **Example 2. SFTP**

  ```
  sftp sftp://user1@OTHER.REALM@vmsnode1.mycompany.com
  ```

- **Example 3. SCP**

  ```
  scp c:\temp\somefile.txt scp://user1@OTHER.REALM@vmsnode1.mycompany.com
  ```

WinSCP for Windows

- The interactive login window accepts a Kerberos principal name in the **Username:** field.
- Command line options:

- The **WINSCP** command supports the URI format noted above.
- The Kerberos principal name can be specified with the ***/username*** option:

```
WINSCP /username:user1@OTHER.REALM vmsnode1.mycompany.com
```

PuTTY for Windows

- By default, PuTTY prompts for a username and accepts a Kerberos principal name (no quotes required).
- From the command line, use the **-l** option to specify the Kerberos principal name:

```
putty -l user1@OTHER.REALM vmsnode1.mycompany.com
```

OpenSSH for Linux

- SSH client

  Use the **-l** option or specify the Kerberos principal name within tick (single quote) characters:

```
ssh -l user1@OTHER.REALM vmsnode1.mycompany.com
ssh 'user1@OTHER.REAL'@vmsnode1.mycompany.com
```

- SFTP and SCP clients

  Specify the Kerberos principal name within tick characters:

```
sftp 'user1@OTHER.REALM'@vmsnode1.mycompany.com
scp ./localfile.txt 'user1@OTHER.REALM'@vmsnode1.mycompany.com:
```

Password Changes

- To allow users authenticated through external authentication to change their Windows account password when it has expired, include the kpasswd_server tag in the appropriate realm subsection (within the [REALMS] section) of KRB5.CONF. Specify the desired target KDC host as the value; for example:

```
[REALMS]
          COMPANY.COM  = {
                         kdc = kerberos1.company.com
                         kpasswd_server = kerberos1.company.com
                                                              …
                                    }
```

- Users who successfully login using external authentication may change their Windows account password using the DCL **SET PASSWORD** command.
- If neither kpasswd_server nor admin_server (with port 464) is present in the realm section of KRB5.CONF, the following **SET PASSWORD** error occurs:

```
$ SET PASSWORD
Old password:
New password:
Verification:
**** The New Password was not accepted ****
```

```
%ACME-F-FAILURE, operation failure; if logging is enabled, see details
 in the ACME$SERVER log file
```

- TCP/IP for OpenVMS SSH user sessions also require the following system logical name be defined:

  ```
  $ DEFINE /SYSTEM TCPIP$SSH_SERVER_USE_LOGINOUT 1
  ```

  If the logical name is not defined, the **SET PASSWORD** command fails after entering the current password with the following error:

  ```
  $ SET PASSWORD
  Old password:
  %SET-F-PWDNOTVAL, old password validation error; password not changed
  ```

7. Supporting Multiple Realms

To support Kerberos authentication for users from multiple realms, information for each additional realm must be included in the KRB5.CONF file:

- A new realm subsection must be added to the [REALMS] section which contains one or more kdc tags to designate the KDCs of the realm. For example, to add the realm named OTHER.REALM:

  ```
  [realms]
              OTHER.REALM = {
                            kdc = kerberos1.other.realm
                            kdc = kerberos2.other.realm
                            admin_server = keberos1.other.realm
                            kpasswd_server = kerberos1.other.realm
                            }
  ```

- A new auth_to_local rule must be added in the default realm's subsection (not in the subsection of the new realm). This rule maps users from the OTHER.REALM realm to local usernames by stripping the @OTHER.REALM portion from the Kerberos principal name. For example:

  ```
  auth_to_local = RULE:[1:$1@$0](.*@OTHER.REALM)s/@.*//
  ```

Note

When one or more auth_to_local rules are defined, the DEFAULT rule must also be explicitly defined for principal name mapping to function correctly. For example, to allow users with a Kerberos account in both the default realm and the OTHER.REALM realm to log in using external authentication, both of the following rules are required:

```
auth_to_local = RULE:[1:$1@$0](.*@OTHER.REALM)s/@.*//
auth_to_local = DEFAULT
```

Note

For information about the auth_to_local rule components, refer to the MIT Kerberos KRB5.CONF documentation [https://web.mit.edu/Kerberos/krb5-1.12/doc/admin/conf_files/krb5_conf.html].

8. Username Mapping

Kerberos for OpenVMS supports both implicit and explicit username mapping. Implicit mapping, however, is limited to users of the default realm only when the KRB5.CONF contains no auth_to_local

username mapping rules. Implicit username mapping also requires the user's Windows username and OpenVMS username be identical. In all other cases, explicit username mapping is required as described below.

Two KRB5.CONF tags are used to implement explicit username mapping: auth_to_local and auth_to_local_names. Both should be placed in the default realm subsection within the [REALMS] section.

- The auth_to_local tag specifies rules for deriving an OpenVMS username from a Kerberos principal name. Typically, these rules remove the @REALM portion of the principal name, leaving only the Kerberos username to be used as the OpenVMS username. A default rule, named DEFAULT, removes the @REALM portion of the principal name for users in the default realm. If KRB5.CONF contains no auth_to_local rules, the DEFAULT rule is applied implicitly. However, if one or more auth_to_local rules are defined in KRB5.CONF, the DEFAULT rule must also be explicitly specified to enable username mapping for users in the default realm. When specifying multiple auth_to_local rules, place each rule on a separate line containing the auth_to_local tag. For example:

  ```
  auth_to_local = <Rule1>
  auth_to_local = <Rule2>
  ```

  In general, auth_to_local tags are necessary only when multiple realms are defined in (the [REALMS] section of) KRB5.CONF. See the *Section 7, "Supporting Multiple Realms"* section above for further information.

- Use the auth_to_local_names subsection to explicitly map Kerberos (Windows) principal names to OpenVMS usernames, when the usernames are not identical. Mappings in the auth_to_local_names subsection take precedence over rules defined by the auth_to_local tags. Specify one mapping per line. For example:

  ```
  auth_to_local_names = {
  windowsusername1 = VMSusername1
  windowsusername2 = VMSusername2
                                …
                          }
  ```

When specifying the Windows username:

- Do not include the realm name.
- Use the correct case (typically all lowercase), because Kerberos usernames are case-sensitive.
- The OpenVMS username is not case-sensitive.

9. Miscellaneous Information

Starting with Windows Server 2025, Kerberos no longer honors the legacy SupportedEncryptionTypes registry value (REG_DWORD) located at:

```
HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Lsa\Kerberos\Parameters
```

Microsoft recommends using group policy instead.

In mid-2026, Microsoft will disable RC4 by default for Kerberos authentication in Windows Server 2008 and later. AES-SHA1 will become the minimum supported encryption type for Kerberos authentication.

If a user's Active Directory account is locked, the following KINIT error occurs:

```
$ kinit aduser1
KRB$KINIT(v5): Clients credentials have been revoked
while getting initial credentials
```

Systems Running Samba for OpenVMS

- Samba for OpenVMS supports Kerberos authentication but does not use the Kerberos for OpenVMS product.
- When configured as a domain member server (only), Samba for OpenVMS uses a built-in Kerberos library based on Heimdal Kerberos.
- The Kerberos configuration file for Samba for OpenVMS is SAMBA$ROOT:[VAR.LOCK.SMB_KRB5]KRB5.CONF_*domain-name*.
- The default Kerberos configuration file for Kerberos for OpenVMS is KRB$ROOT:[ETC]KRB5.CONF.
- While Kerberos for OpenVMS and Heimdal Kerberos share some configuration parameters, they are not compatible and should be maintained separately.
- Both Kerberos for OpenVMS and Heimdal Kerberos use the same logical name – KRB5_CONFIG – to specify the location of the Kerberos configuration file. Defining this logical name incorrectly can cause unexpected behavior.
- When an OpenVMS process executes the following command:

  ```
  $ @SAMBA$ROOT:[BIN]SAMBA$DEFINE_COMMANDS
  ```

  Samba defines KRB5_CONFIG as a process logical name which equates to the Heimdal-compatible KRB5.CONF file used by Samba. This process logical name definition is required only if the OpenVMS process executes Samba commands such as **`NET ADS`** and **`SMBCLIENT`**. The process logical name should be deassigned if the process intends to use the Kerberos for OpenVMS product.

KDC Failover Time

When a realm section in KRB5.CONF contains multiple kdc tags, the Kerberos for OpenVMS client application will attempt to connect to the first KDC listed. If this KDC is unreachable, by default, the connection attempt will timeout after 75 seconds before attempting to connect to the next KDC. To decrease the time to fail over to the next KDC, reduce the value of the TCP/IP Services for OpenVMS INET subsystem tcp_keepinit configuration parameter to a value less than 15 seconds.

Note

Note that the values are expressed in units of half seconds, so the default value of 150 is 75 seconds. For example, to set the timeout on the running system to 10 seconds:

```
$ TCPIP SYSCONFIG -r INET TCP_KEEPINIT=20
tcp_keepinit: reconfigured
```

To retain the setting across TCP/IP for OpenVMS restarts and system reboots, set the TCP_KEEPINIT parameter in the system configuration table TCPIP$ETC:SYSCONFIGTAB.DAT. Use the SYSCONFIGDB utility to update TCPIP$ETC:SYSCONFIGTAB.DAT (do not modify TCPIP$ETC:SYSCONFIGTAB.DAT using other methods).

To update the system configuration table:

1. Create a stanza file, for example, INET-TCP_KEEPINIT.STANZA, which contains the name of the subsystem (INET) and the parameter setting. For example, to set TCP_KEEPINIT to 20 (10 seconds), add the following lines and save the file:

   ```
   inet:
   tcp_keepinit=20
   ```

2. Merge the stanza file into the existing system configuration table using the **-m** option:

   ```
   $ TCPIP SYSCONFIGDB -m INET -f INET-TCP_KEEPINIT.STANZA
   ```

kpasswd Configuration

The **kpasswd** command requires the admin_server tag.

The **kpasswd** command uses the KDC specified by the admin_server tag in the appropriate realm subsection of the [REALMS] section of KRB5.CONF. For Windows KDCs, port number 464 must also be specified. For example:

```
admin_server = kerberos1.company.com:464
```