BCAAA 6.1
Service Requirements

Current Version: 6.1.5

Guide Revision: 9/17/2020

Symantec

Contents

BCAAA 6.1 Service Requirements

This document describes the BCAAA compatibility and upgrade/downgrade requirements for SGOS versions that use BCAAA 6.1.

Version Information

Current Version: 6.1.5
SGOS Compatibility: SGOS 5.4, 5.5, 6.x, 7.x
Platform Compatibility: Windows Server 2008, 2012, 2016, and 2019

About BCAAA

Symantec's Authentication and Authorization Agent (BCAAA) allows SGOS to manage authentication and authorization for several different authentication methods. BCAAA is a software agent that acts as an intermediary between the ProxySG appliance and the authentication domain. The agent is installed on a domain controller or member server and is configured separately from SGOS.

> **Caution:** Running BCAAA on a server with other responsibilities can cause performance issues, leading to network outages. Symantec recommends that you install the agent on a dedicated domain controller or member server, reserved for the purpose of managing authentication between the appliance and the domain.

The BCAAA service acts as an intermediary service between the ProxySG appliance and the following authentication schemes:

- Integrated Windows Authentication (IWA)
- SiteMinder
- Windows SSO
- Novell SSO

To use BCAAA, you must first download the agent from MyBroadcom.

> **Note:** For details on downloading BCAAA and other Symantec software, refer to https://knowledge.broadcom.com/external/article/151364/download-the-latest-version-of-symantec.html.

For information on SGOS releases, refer to the *SGOS Release Notes* that correspond to the SGOS version to which you are upgrading.

Important Installation Prerequisites

This section provides important notes and actions that should be completed before beginning BCAAA installation.

Step One: Read Supporting Information

Before starting BCAAA installation, read the *SGOS Release Notes* (if you are upgrading or downgrading) and the SGOS Upgrade/Downgrade Guide.

Step Two: Verify Supported Authentication Methods, Platforms, and Directory Service Operating Systems

See "Supported Authentication Methods" on page 8 and "The Supported Platforms and Directory Services Operating Systems" on page 9.

Step Three: Identify the Appliance BCAAA is to be Installed on

Running BCAAA on a server with other responsibilities can cause performance issues, leading to network outages. Symantec recommends that you install the agent on a dedicated domain controller or member server, reserved for the purpose of managing authentication between the appliance and the domain.

If the agent is installed on a non-dedicated server, user experience can suffer because the BCAAA server is in the client data path for accessing protected resources. Users make client requests to the ProxySG, which in turn proxies authentication requests to the BCAAA service. If the BCAAA service has to compete for system resources, the BCAAA response to the authentication request could take longer.

Step Four: Verify Disk Space

See "BCAAA Disk Space Requirements" on page 7.

Step Five: Check BCAAA Support and Installation Requirements

BCAAA 6.1 introduces changes in BCAAA installation. All previous BCAAA installations must be deleted before installing BCAAA 6.1. The uninstall process retains the .ini files from previous BCAAA installations to preserve any customer changes.

Before upgrading to, or downgrading from your current SGOS version, you must first ensure that the target release is compatible with BCAAA 6.1. If the release requires a different BCAAA version, you must uninstall BCAAA 6.1 and install the BCAAA version required for the release you are migrating to. For example, if you plan to downgrade to a pre-SGOS 5.4 release, you must uninstall BCAAA 6.1 and install the required BCAAA before installing SGOS.

The SGOS upgrade/downgrade procedure is described in the SGOS Upgrade/Downgrade Guide; refer to the appropriate document for your SGOS version.

Step Six: Plan Downtime

While installing or upgrading BCAAA, stop the service to allow files to be copied during the installation process. If you have configured an alternate BCAAA server, the ProxySG appliance will fail over to that server when BCAAA is stopped. If you have not configured an alternate BCAAA server, you must schedule downtime to perform the installation.

Step Seven: Create a Domain User account (IWA/Kerberos Only)

(Optional) If you plan to use BCAAA for IWA/Kerberos, or Windows SSO, you must create a domain user account for the BCAAA service in the Windows Active Directory (AD).

BCAAA Disk Space Requirements

To install BCAAA, make sure that you have at least 45 MB of disk space on your Windows server. Although some versions of BCAAA might require less than 45 MB of disk space, allocating 45 MB of disk space will address the needs to complete the BCAAA installation process.

Additional space might be required, depending on the features that have been enabled.

- If using Windows SSO with Domain Controller Query

  Add 256 bytes for each concurrent login. For example, if 1000 users will be concurrently logged in to theWindows domain during peak hours, then this feature requires 256k (256 bytes record * 1000 concurrently logged in users).

- If using Novell SSO

  Add 256 to 512 bytes for each user concurrently logged in to Novell eDirectory. You only need to count users that are in containers that are monitored by a Novell SSO realm.

For Novell SSO, the record length is dependant on the length of each user's distinguished name in eDirectory. Users with long distinguished names require extra storage. Because distinguished names have a maximum length of 256 bytes in eDirectory, an individual Novell SSO record will not be larger than 512 bytes.

Supported Authentication Methods

BCAAA acts as an intermediary service between the ProxySG appliance and the following authentication methods. Refer to the *SGOS Administration Guide* for information about configuring these authentication methods

CA SiteMinder

When a SiteMinder realm is referenced in policy, a BCAAA process is created. The ProxySG then sends a configuration request that describes the servers to use. The BCAAA service logs in to the appropriate servers and determines configuration information to be passed back to the ProxySG appliance (such as the kind of credentials required). Responses from the SiteMinder policy servers are translated into appropriate BCAAA protocol responses and returned to the appliance.

Before you can use the BCAAA service with SiteMinder, you must configure the appropriate ProxySG realm to work with the SiteMinder servers. The realm can be configured from the SiteMinder configuration tabs in the Management Console or from the CLI.

> **Note:** Each (active) SiteMinder realm on the ProxySG must reference a different agent on the Policy Server.

IWA

For IWA, the BCAAA service is installed on a domain controller or member server and usesWindows APIs to authenticate the user and obtain group information.

- The BCAAA service uses an Integrated Windows Authentication (IWA) to authenticate a user with Active Directory. When using IWA, the realm and (IWA) authentication challenges are used.
- NTLM: NTLM is a subset of IWA.
- Kerberos: Kerberos is the default network authentication protocol used in Windows 2000 and later.When using Kerberos the BCAAA service must share a secret with a Kerberos server (called a KDC) and register an appropriate Service Principal Name (SPN).

Novell SSO

The BCAAA service manages communication with the Novell eDirectory server.

Windows SSO

The BCAAA service is used to supply mappings for IP addresses to logged on users. TheWindows SSO realm can use domain controller querying, or client querying, or both domain controller and client querying to determine the logged-on user. Domain controller querying is enabled automatically in BCAAA 6.1.

The Supported Platforms and Directory Services Operating Systems

The following table describes the platforms that BCAAA 6.1 can run on to support the specified authentication method. The supported operating systems for your directory services are identical to the list of supported platforms.

BCAAA can run on any hardware as long as the specified operating system requirements are met. For virtual machine deployments on Windows, see the appropriate documentation for your Windows platform and the virtual machine software to ensure compatibility.

Supported Platforms and Directory Service Operating Systems	Supported Authentication Methods			
	Integrated Windows Authentication	CA eTrust SiteMinder version 5.5 and 6.0	Windows SSO	Novell SSO
Windows® Server 2019	✓	✓	✓	✓
Windows® Server 2016	✓	✓	✓	✓
Windows® Server 2012	✓	✓	✓	✓
Windows® Server 2012 Read-Only	✓	✓	✓	✓
Windows® Server 2012 R2	✓	✓	✓	✓
Windows® Server 2012 R2 Read-Only	✓	✓	✓	✓
Windows® Server 2008 R2	✓	✓	✓	✓
Windows® Server 2008 R2 Read-Only	✓	✓	✓	✓

Windows® Server 2008 (32- and 64-bit)	✓	✓	✓	✓
Windows® Server 2008 Read-Only	✓			

Note: If the BCAAA log displays the message "Cannot query domain controller <*IP_address*>; status=5:0x5:Access is denied" when using Windows Server 2019, your deployment requires additional configuration steps; refer to KB article 194792 for instructions.

Note: BCAAA can be run directly on a server or on a server that is also acting as a domain controller. For better performance, use a dedicated server for the BCAAA installation.

Install BCAAA

The following procedure describes how to install BCAAA on a Windows system. Refer to the release notes for information on supported Windows platforms.

Step One: Perform Pre-Installation Tasks

See "Important Installation Prerequisites" on page 5.

Step Two: Download BCAAA

1. Log in (as a user with administrative privileges) to the Windows server where you plan to install BCAAA. Administrative privileges are required to perform BCAAA installation but are not required for BCAAA users.
2. Download the BCAAA setup package from one of the following locations:
   - ProxySG Management Console (**Configuration >Authentication > IWA > IWA Servers**)
   - MyBroadcom

   > **Note:** For details on downloading BCAAA and other Symantec software, refer to https://knowledge.broadcom.com/external/article/151364/download-the-latest-version-of-symantec.html.

Step Three: Install BCAAA

1. Uninstall all previous BCAAA instances before installing version 6.1.

   If you try to install BCAAA version 6.1 before removing the previous version, you will receive an error. For help, refer to KB article 165481.
2. Unzip the BCAAA Setup file and double-click the .exe file to launch the BCAAA Setup.
3. To begin the setup, click **Next**.
4. Specify a destination folder for the BCAAA software.

   You can accept the default location (C:\Program Files\Blue Coat Systems\BCAAA) or browse to a different location. Make sure that anti-virus software is not configured to scan the directory where you install BCAAA. Click **Next** to continue.

> **Note:** If you are installing on a system that had a previous BCAAA installation, make sure you install to the same location as the previous version to ensure that your configuration settings are retained.

5. Specify the Port Number that BCAAA and the ProxySG appliance will use to communicate.

   By default, both BCAAA and the ProxySG appliance use 16101. If you choose a port other than the default, you must set the same value on the ProxySG appliance.

   If the specified port is blocked by your server's firewall, the installer asks if would like it to be opened. You must also make sure that this port is not blocked, for example by another firewall between the BCAAA server and the ProxySG appliance. Click **Next** to continue.

6. Select one of the following options to specify whether you want to use SSL between the ProxySG appliance and BCAAA:

   - **Permitted**–Both SSL and non-SSL connections can be used.
   - **Required**–BCAAA and the ProxySG appliance can only connect using SSL.
   - **Forbidden**–SSL can not be used between BCAAA and the ProxySG appliance.

   The SSL settings on the ProxySG appliance and BCAAA must match. After you make a selection, click **Next**.

7. If you selected **Permitted** or **Required**, you will be prompted for the following SSL configuration information:

   - **Certificate Subject**–Enter the hostname of the server where you are installing BCAAA; do not use the IP address. Your DNS server must be able to resolve the hostname you supply. Click **Next** to continue. The installation program checks to see if the server's certificate store already contains a certificate with this subject name. If it does not find one, it automatically generates a new self-signed certificate with the specified subject name.
   - **Save the automatically generated certificate in the certificate store?**–Select **Yes** and then click **Next** to continue. Note that this option only appears if the BCAAA installation generated a new self-signed certificate.
   - **Require the ProxySG to provide a valid certificate in order to connect?**–If you want to use mutual SSL between BCAAA and the ProxySG, select **Yes**. Otherwise, select **No**.

   After you make your selection, click **Next** to continue.

8. Indicate whether the BCAAA installation will support a ProxySG appliance appliance using a Windows SSO realm or a PacketShaper.

- Select **No** if you are using BCAAA with Novell SSO, SiteMinder, IWA/Basic, IWA/NTLM.
- Select **Yes** if:
  - You are using BCAAA withWindows SSO or a PacketShaper.
  - You are using BCAAA withWindows SSO and for one of the other realms (SiteMinder, IWA/Basic, IWA/NTLM).

After you make your selection, click **Next**. If you selected **Yes**, you will be prompted for the User Name and Password for the domain user you created in "Important Installation Prerequisites" on page 5.Note that the user name you supply must include the domain name (for example, mydomain\bcaaa_user or bcaaa_user@mydomain.com).

9. If you selected **No** in Step 8, you must now specify whether to run BCAAA as the LocalSystem account or as a domain user. If you are using BCAAA with IWA/Kerberos, or Kerberos Constrained Delegation, select **Yes**. After you make your selection, click **Next**. If you selected **Yes**, you will be prompted for the User Name and Password for the domain user you created in "Important Installation Prerequisites" on page 5.

   When installation is complete, the installer displays the final BCAAA dialog.

Uninstalling or Modifying the BCAAA Service

To modify the BCAAA installation, uninstall and reinstall it.

To uninstall the authentication agent:

1. Launch the install wizard.
2. Click **Next** to start the procedure.
3. Click **Finish** to exit the uninstall application.

> **Note:** For help with uninstalling previous BCAAA versions, refer to KB article 165481.

Troubleshoot BCAAA

The following topics describe common BCAAA problems and solutions.

Troubleshoot Authentication Agent Problems

This topic describes some common problems you might encounter when setting up or using the BCAAA service on a Windows platform.

To troubleshoot the BCAAA service, launch the event viewer:

1. In Windows, click the **Start** button.
2. In the Search box, type **Event Viewer**.

The Properties pane displays, providing information about the status of the BCAAA service at that time. Notice the Type and the Event ID. The description below the **Type/Event ID** lists the problem. You can often find more information about the problem and suggestions for its solution in "Common BCAAA Event Messages" on page 22.

Common problems:

- If an attempt to start the BCAAA service is issued when BCAAA is already started, the following error message displays: `The requested service has already been started.`
- If another application is using the same port number as the BCAAA service, the following messages are displayed:

```
The BCAAA service could not be started.
A system error has occurred. System error 10048 has occurred.
Only one usage of each socket address (protocol/network address/port) is normally permitted.
```

- Active Directory Distribution groups are not supported by BCAAA for IWA realms. IWA realms only support Security Groups or testing against individual users.

View or Modify BCAAA Service Properties

To modify BCAAA service properties:

1. Launch the Windows Service Control Manager:

    a. Click **Start** in Windows.

    b. In the **Run** area, enter **services.msc**.

    c. Press **Enter**.

    The Windows Service Control Manager displays.

2. Right-click on the BCAAA service and select **Properties** to manage the service.

    For example, to make the BCAAA service start only manually, set the Startup Type to **Manual**. (Automatic is the default setting.)

Troubleshoot SSL Support

Issue: The existing BCAAA connection over SSL fails in SGOS 6.7.1.

In SGOS 6.7.1, the TLS defaults are v1.1 and v1.2, which may not be supported by an older Windows server's SSL setting for the BCAAA connection.

Solution: Enable TLSv1 on the default SSL device profile.

> **Note:**
> - Windows XP and Windows Server 2003 do not support TLS 1.1 or TLS 1.2.
> - Windows Vista and Windows Server 2008 do not support TLS 1.1 or TLS 1.2.

> **Caution:** If you are using a Windows version later than those listed here, do not edit the default SSL device profile.

Issue: The BCAAA service fails to negotiate an SSL connection under certain conditions when the BCAAA user is changed.

Solution: Give the BCAAA user access to the certificate store.

Stop the BCAAA service. From the Run prompt, launch the regedit program to give the BCAAA user full access to the following key and its children:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Services
```

Troubleshoot Authentication Agent Problems

This topic describes some common problems you might encounter when setting up or using the BCAAA service on a Windows platform.

To troubleshoot the BCAAA service, launch the event viewer:

1. In Windows, click the **Start** button.
2. In the Search box, type **Event Viewer**.

The Properties pane displays, providing information about the status of the BCAAA service at that time. Notice the Type and the Event ID. The description below the **Type/Event ID** lists the problem. You can often find more information about the problem and suggestions for its solution in "Common BCAAA Event Messages" on page 22.

Common problems:

- If an attempt to start the BCAAA service is issued when BCAAA is already started, the following error message displays: `The requested service has already been started.`
- If another application is using the same port number as the BCAAA service, the following messages are displayed:

```
The BCAAA service could not be started.
A system error has occurred. System error 10048 has occurred.
Only one usage of each socket address (protocol/network address/port) is normally permitted.
```

- Active Directory Distribution groups are not supported by BCAAA for IWA realms. IWA realms only support Security Groups or testing against individual users.

Determine the BCAAA Version

Fixes are sometimes included in later BCAAA release versions. Use one of the following methods to determine the BCAAA version running on the authentication server:

Control Panel

Complete the following steps:

1. Click **Start** > **Control Panel**.
2. Click **Programs** and **Features**.
3. After the list populates, find BCAAA and read the version number listed in the **Version** column.

Program Files

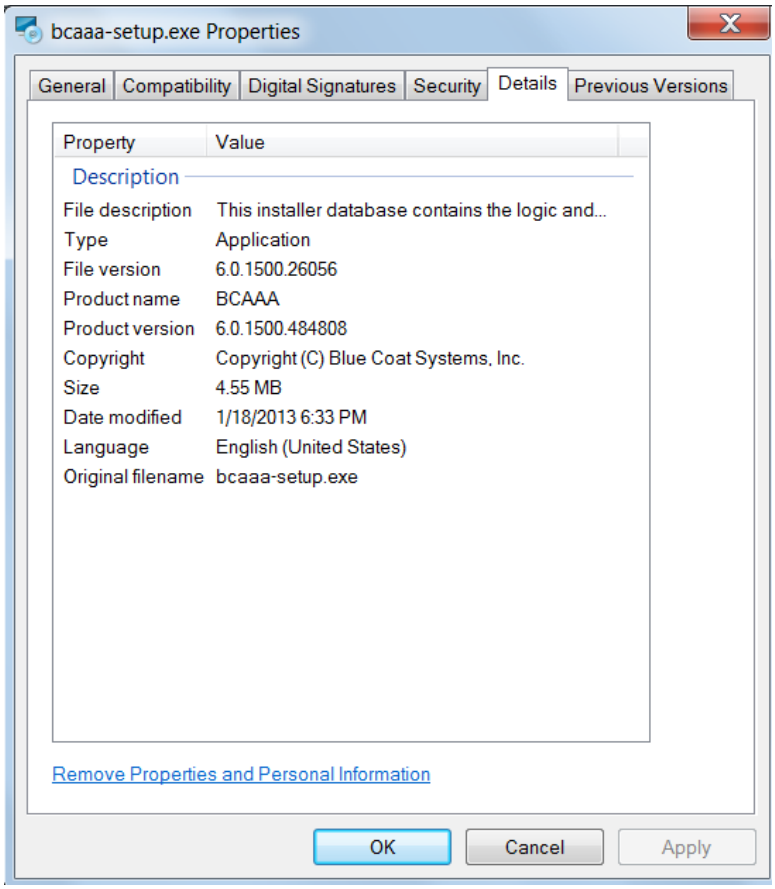
Complete the following steps:

1. Go to the folder where the bcaaa-setup.exe resides. For example:

   ```
   C:\Program Files\Blue Coat Systems\BCAAA
   ```

2. Right click the bcaaa-setup.exe file, select **Properties**, and click the **Version** tab. (In Windows 2008, click the Properties and Details tab.)

Refer to the following example:



Common BCAAA Event Messages

The following table describes the common BCAAA event messages logged to the Windows Application Event Log. Most of the event messages not listed here are error status messages returned by Win32 function calls. When a Win32 call fails, the error code and error text containing the reason for the error displays in the event log under the name BCAAA.

View the application event log

To view the BCAAA event log:

1. Right click on My Computer and select **Manage**.
2. Select **System Tools > Event Viewer > Application**.

For each BCAAA event message, the event message is displayed along with the event number.

Message ID	Message	Description
200	Various messages	Provides information about a condition that is not an error.
300	Various messages	Warns about an unexpected condition that does not prevent operation.
400	Various messages	Describes an error condition that prevents normal operation.
1001	`Authentication Agent service started: port=# threads=# socket=0x# process id=# agent version=# remote appliance version=#`	Indicates successful startup and provides information about the agent.
1002	`Authentication Agent stopped`	Indicates normal shutdown of the service.
1003	`remote appliance (a.b.c.d) connected; Process # spawned as #`	Indicates that a ProxySG has connected to the agent (Windows only).
1004	`remote system agent process exited (normal logout)`	Indicates normal logout by a ProxySG.
1005	`Process %d has terminated, ExitCode=0x#, link=0x#`	Indicates an unexpected termination of an agent process (Windows only).
1006	`Service dispatcher exited.`	Indicates an unexpected termination of the service dispatcher.
1007	`CreateNamedPipe failed, pipe='%s'`	The agent dispatcher could not create the named pipe for the reason given.

Message ID	Message	Description
1008	`ConnectNamedPipe failed, pipe='%s'`	The agent process could not obtain the information from the dispatcher on the named pipe for the reason given.
1009	`WriteFile failed, pipe='%s'`	The dispatcher could not write information to the named pipe for the reason given.
1011	`CreateThread (ProcessTimerThread) failed`	The dispatcher could not create its timer thread.
1012	`Failed to create ProxySG process '%s'`	The BCAAA server does not have the same version of BCAAA available as the ProxySG is expecting.
1019	Various messages	The dispatcher was unable to determine the exit status of an agent process.
1020	`Terminating remote system process #, ProcNum=# Handle=0x#`	An agent process was active when the Windows service was shut down.
1022	Various messages	The associated message reports the status of a ProxySG login attempt.
1101	BasicAuth: CloseHandle failed; user 'xx\\xx'	The agent was unable to close the login handle for the specified user.
1102	`Username: '%s\\%s' too long`	The ProxySG offered the specified username, which is too long.
1106	Various messages	An attempted authentication using BASIC credentials failed for the reason given.
1107	`User Right 'Act as part of the operating system' required for Basic Authentication`	The agent does not have the necessary privileges to do BASIC authentication
1108	Various messages	The agent was unable to determine information about the user for the reason given.
1202	`Unable to create GroupsOfInterest mutex 'xx' - already exists`	The agent could not create the Windows mutex needed for group authorization checks because it already exists.
1203	`Unable to create GroupsOfInterest mutex 'xx`	The agent could not create the Windows mutex needed for group authorization checks.
1204	`OpenMutex failed for AuthGroups mutex '%s', group='%s'`	The agent was unable to open the Windows mutex needed for group authorization checks.
1205	Various messages	The agent was unable to close the Windows mutex named for the reason given.
1207	`GetAclInformation failed`	The agent was unable to obtain ACL information needed to do group authorization checks.
1209	`GetKernelObjectSecurity failed for AuthGroup='%s'`	The agent was unable to obtain security information about the specified group.

Message ID	Message	Description
1210	`SetKernelObjectSecurity failed`	The agent was unable to set up security information for the reason specified.
1211	`InitializeSecurityDescriptor failed`	The agent was unable to initialize the security descriptor for the reason specified.
1212	`GetSecurityDescriptorDacl failed`	The agent was unable to get the discretionary access control list (DACL) for the reason specified.
1213	`SetSecurityDescriptorDacl failed`	The agent was unable to set the discretionary access control list (DACL) for the reason specified.
1214	`InitializeAcl failed`	The agent was unable to initialize the access control list (ACL) for the reason specified.
1215	`GetUserName failed for AuthGroup='%s'`	The agent was unable to determine the username while processing the specified group.
1217	`GetAce failed for AuthGroup='%s'`	The agent was unable to get the access control entry (ACE) for the specified group.
1218	`AddAce failed`	The agent was unable to add the necessary access control entry (ACE) for the reason specified.
1219	`AddAccessAllowedAce failed`	The agent was unable to add the necessary "access allowed" access control entry (ACE).
1220	`Could not establish groups-ofinterest: result=0x##`	The agent was unable to initialize groups-of-interest checking.
1221	`AuthGroup '%s' does not exist`	The specified group does not exist.
1222	`IWA RevertSecurityContext failed, user='%s'`	The agent could not revert the security context for the specified user.
1223	`BASIC: RevertToSelf failed, user='%s'`	The agent could not revert the security context for the specified user.
1224	`Error calling OpenProcessToken`	The agent's call to `OpenProcessToken` failed for the specified reason.
1225	`Error calling LookupPrivilegeValue`	The agent could not get information about a needed privilege.
1226	`Error calling AdjustTokenPrivileges`	The agent could not adjust its privileges as required.
1227	`ImpersonateLoggedOnUser failed; Group access denied for user '%s'`	The agent could not impersonate the specified user.
1228	`IWA: ImpersonateSecurityContext failed; Group access denied for user '%s'`	The agent could not impersonate the specified user.
1301	`NOTE: Pending ContextLink=### timed out; deleting SecurityContext h=## TS=## now=##`	The ProxySG did not provide a response to a challenge quickly enough.

Message ID	Message	Description
1302	Various messages	An authentication request from a ProxySG referenced an in-progress request that has timed out or does not exist.
1304	Various messages	The agent was unable to delete a security context for the reason given.
1305	`AcceptSecurityContext failure, SEC_E_ INVALID_HANDLE, ContextLink=### count=#`	The agent was provided with an invalid context handle.
1306	Various messages	The client provided an invalid token to the authentication system.
1308	`AcceptSecurityContext failure, ContextLink=# count=#, detail=#(xxx)`	Windows rejected the authentication attempt for the reason given.
1310	Various messages	Records the failure of NTLM authentication or group authorization.
1311	`3:Failed NTLM Authentication for user: '%s'`	Records the failure of NTLM authentication; the user name was supplied by the client.
1312	Various messages	The agent could not determine the username from the NTLM type 3 message supplied by the client.
1313	`Invalid Type3 message`	The client provided an NTLM type 3 message that was invalid.
1314	`BASE64_Decode: Length of token exceeds max (%d)`	The client provided an NTLM token that was too long.
1316	`Unsupported version in request: %d(0x%x)`	The ProxySG sent a request with an unsupported version number.
1401	Various messages	The agent lost communication with the ProxySG.
1402	`Unexpected thread 0 exit`	The agent exited unexpectedly.
1403	Various messages	The agent is aborting for the reason given.
1404	`Unable to get ProcessInfo from parent process.`	The agent could not obtain its information from the dispatcher.
1405	`CreateFile failed, pipe='xx'`	The agent could not create a handle for the dispatcher's named pipe.
1406	`WaitNamedPipe failed, pipe='%s'`	The agent could not wait for the dispatcher's named pipe.
1407	`ReadFile failed, pipe='%s'`	The agent could not read information from the dispatcher's named pipe.
1409	Various messages	The agent could not create the specified thread for the reason given.

Message ID	Message	Description
1412	Various messages	The agent could not create a required Windows event object.
1413	`AuthMethod 'xxs' not supported: returning _AuthResult=0x##`	The ProxySG requested an unsupported authentication mechanism.
1414	Various messages	The specified request is unsupported.
1500	Various messages	The agent has a problem with memory allocation; typically this means there is not enough memory.
1501	`Unable to allocate memory for ProcLink buffer.`	The agent could not allocate some needed memory.
1502	`Unable to allocate memory for ContextLink buffer.`	The agent could not allocate some needed memory. 1503 Various The agent was unable to allocate needed memory.
1604	`Service dispatch failed`	The Windows service dispatcher failed to start.
1605	`RegisterServiceCtrlHandler failed`	The agent dispatcher was unable to register the service control handler.
1608	`SetServiceStatus failed, g_StatusHandle=%d`	The agent was unable to set the service's status.
1610	`Unsupported service control code: #`	Windows sent a service control code that the agent does not support.
1701	`WSASocket failed`	The agent could not create a Windows socket for the reason given.
1702	`WSAStartup failed.`	The agent could not start the Windows socket for the reason given.
1703	Various messages	The agent could not send data to the ProxySG for the reason given.
1704	Various messages	The agent could not receive data from the ProxySG for the reason given.
1705	`accept failed`	The agent dispatcher could not initialize to accept new connections.
1706	`bind failed, PortNumber=#`	The agent dispatcher could not bind to the specified port.
1707	`listen failed.`	The agent dispatcher could not listen for new connections.
1708	Various messages	Windows reported an event wait failure to the agent while doing I/O on the socket.

Message ID	Message	Description
1709	`The agent is already running or the agent's port # is in use by another process`	Some other process is already using the port needed by the agent.
1710	`WSARecv failed reading bytes from socket`	Windows reported an error when the agent tried to receive bytes from the ProxySG.
1711	`WSASend failed sending bytes to socket.`	Windows reported an error when the agent tried to send bytes to the ProxySG.
1712	Various messages	A socket I/O operation did not complete successfully.
1801	`Error calling AcquireCredentialsHandle`	The agent could not acquire its credentials from Windows.
1803	Various messages	The agent could not load a needed library (DLL).
1804	Various messages	The agent could not locate the needed services in a library (DLL).
1805	`Unsupported SSPI Windows platform; PlatformId=#`	The reported Windows platform is not supported for NTLM authentication.
1806	`Error calling QueryContextAttributes`	The agent could not determine the authenticated user's security attributes.
1807	`QuerySecurityPackageInfo failed`	The agent could not get needed security information from Windows.
1808	`Max Token size too long (#); max size is #`	The client supplied an NTLM token that is too long.
1809	`FreeContextBuffer failed`	An attempt to free the NTLM context buffer failed.
1811	`Username 'x\\y' too long`	The reported user name is too long.
1901	`Admin Services Error: Access denied to domain/user/group information`	The agent was unable to access necessary information.
1902	`Admin Services Error: Invalid computer from which to fetch information`	The computer to be used to get security information is invalid.
1903	`Admin Services Error: Group not found`	The requested group could not be found. 1904 Various The reported error was encountered while browsing.
1905	`Admin services error: could not translate context to Unicode`	The requested object for browsing could not be translated to Unicode
1906	`Admin service out of memory`	The browsing service ran out of memory.
1907	`Search request object too long: # > #`	The requested object for browsing is too long.

Message ID	Message	Description
2000	`AcquireCredentialsHandle failed: 0x#`	The agent could not acquire the credentials needed for an SSL session.
2001	Various messages	The agent was unable to negotiate an SSL session for the reason given.
2002	Various messages	An I/O error occurred during an SSL session.
2003	Various messages	The specified cryptographic error occurred during an SSL session.
2004	Various messages	The specified problem occurred with a certificate during SSL negotiation.
2204	`Cannot create incremental persistence file; status=3:0x3:`	The system cannot find the path specified. The local computer might not have the necessary registry information or message DLL files to display messages from a remote computer. You might be able to use the /AUXSOURCE= flag to retrieve this description; see Help and Support for details.
2205	Could not initialize SSO; status=3:0x3:	The system cannot find the path specified. The local computer might not have the necessary registry information or message DLL files to display messages from a remote computer. You might be able to use the /AUXSOURCE= flag to retrieve this description; see Help and Support for details.

Changes in BCAAA 6.1

BCAAA 6.1 introduces the following changes:

- BCAAA v6.0 does not support the COREid realm.
- A Solaris version of BCAAA is no longer provided.
- You must uninstall the previous BCAAA installation before installing version 6.1. If you try to install BCAAA version 6.1 before removing the previous version, you will receive an error.
- A new dialog appears in the installation wizard, asking if a Windows SSO realm or a PacketShaper will be used with this installation. The wizard then branches to different paths depending on the response
- The installer automatically enables Domain Controller Query (DCQ) in the sso.ini file when the user responds yes to the above question. Previously, the user had to set this option manually.
- The Modify and Repair options have been removed from the Installer. To modify the BCAAA installation, uninstall and reinstall.
- BCAAA event log messages now refer to a generic device name (for example, remote appliance) instead of ProxySG.
- BCAAA no longer requires “Act as part of the operating system” privilege for IWA realms.

Changes in 6.1.2

- First release: September 2013.
- BCAAA installation as a Domain User failed on Windows Server 2012 R2. (B#190561).
- 3/4/14: Added support for Windows Server 2012 R2 and 2012 R2 Read-Only

Changes in 6.1.3

- Fixed the CreateProcess vulnerability in this version of BCAAA. (B#193774)
- Fixed an issue where authentication could fail for some SSO users who got logged into an RODC domain in Windows Server 2008. (B#200736)

Changes in 6.1.4

- Added support for Windows Server 2016.

Changes in 6.1.5

- Fixed an issue where BCAAA stopped authenticating requests and became unresponsive when a high number of BCAAA realm processes were created after a network device corrupted the initial data from the proxy to BCAAA. (B#254189)
- IPv6 is now supported for connecting to BCAAA for proxies running SG 6.7.4 or later.

Changes in 6.1.51

- Fixed an issue where BCAAA IWA authentication failed if there was a telnet session open to the BCAAA server on BCAAA's listening port. (BCAAA-3)
- Added support for Windows Server 2019.

> **Note:** If the BCAAA log displays the message "Cannot query domain controller <*IP_address*>; status=5:0x5:Access is denied" when using Windows Server 2019, your deployment requires additional configuration steps; refer to KB article 194792 for instructions.

Additional References

Refer to the following documents for additional information. Additionally, there are a number of articles at the Broadcom Support Portal (https://support.broadcom.com/security).

- *IWA Authentication - Fundamentals and Deployment Guidelines*

  https://knowledge.broadcom.com/external/article/166614

- *Implementing proxy authentication*

  https://knowledge.broadcom.com/external/article/166439

- *What ports do the BCAAA Authentication Agent use?*

  https://knowledge.broadcom.com/external/article/167355

- *How do I configure BCAAA Windows SSO synchronization?*

  https://knowledge.broadcom.com/external/article/166025