

# BCAAA 6.1 Service Requirements

**Current Version: 6.1.5**

**Release Date: 03/2017**

**Document Revision: 3/15/2018**



---

## Contents

---

<b>BCAAA 6.1 Service Requirements</b>	<b>3</b>
Version Information	3
<b>About the Blue Coat Authentication and Authorization Agent (BCAAA)</b>	<b>4</b>
<b>Important Installation Prerequisites</b>	<b>5</b>
<b>BCAAA Disk Space Requirements</b>	<b>7</b>
<b>Supported Authentication Methods</b>	<b>8</b>
<b>The Supported Platforms and Directory Services Operating Systems</b>	<b>9</b>
<b>Install BCAAA</b>	<b>10</b>
<b>Uninstalling or Modifying the BCAAA 6.1 Service</b>	<b>12</b>
<b>Troubleshoot BCAAA</b>	<b>13</b>
<b>Troubleshoot Authentication Agent Problems</b>	<b>14</b>
<b>View or Modify BCAAA Service Properties</b>	<b>15</b>
<b>Troubleshoot SSL Support</b>	<b>16</b>
<b>Troubleshoot Authentication Agent Problems</b>	<b>17</b>
<b>Determine the BCAAA Version</b>	<b>18</b>
<i>Control Panel</i>	18
<i>Program Files</i>	18
<b>Common BCAAA Event Messages</b>	<b>19</b>
View the application event log	19
<b>Changes in BCAAA 6.1</b>	<b>26</b>
Changes in 6.1.2	26
Changes in 6.1.3	26
Changes in 6.1.4	26
Changes in 6.1.5	26
<b>Additional References</b>	<b>27</b>
<b>Copyrights</b>	<b>28</b>

## BCAAA 6.1 Service Requirements

BCAAA 6.1 includes support for additional Symantec products, such as PacketShaper, as well as some performance and reliability enhancements. These latter enhancements rely on the newer APIs provided in Windows Server 2008 and later; these are the only Windows Server versions compatible with this version of BCAA.

Symantec recommends that customers using Windows Server 2008 or later upgrade to BCAA 6.x to take advantage of ongoing software enhancements and support.

The previous version of BCAA, 5.5, which is compatible with Windows Server 2003, will continue to be supported through the end of Microsoft's extended support for Windows Server 2003. BCAA 5.5 is compatible with SGOS 5.4, 5.5, 6.1, 6.2, 6.3, 6.4 and 6.5 releases. For information about installing BCAA version 5.5.x, refer to *BCAAA Service Requirements (Legacy Versions)*.

### Version Information

---

**Current Version:** 6.1.5

**SGOS Compatibility:** SGOS 5.4, 5.5, 6.x

**Platform Compatibility:** Windows Server 2008, 2012, and 2016

**Document Revision:** March 2018

## About the Blue Coat Authentication and Authorization Agent (BCAAA)

The Blue Coat Authentication and Authorization Agent allows SGOS to manage authentication and authorization for several different authentication methods. BCAA 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.

The BCAA 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 BCAA, you must first download the agent from MySymantec: <https://support.symantec.com>.



The first time you download files, you are prompted to install the Download Manager. Follow the onscreen prompts to download and run the installer. For more information, refer to <https://www.symantec.com/support-center/getting-started>.

---

# Important Installation Prerequisites

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

## Step One: Read Supporting Information

Before starting BCAA 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 BCAA is to be Installed on

Blue Coat recommends that the Windows BCAA service be installed on a dedicated Windows machine. Installation of any other non-essential software might degrade the BCAA service performance, which in turn degrades the user experience.

This is because the BCAA 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 BCAA service. If the BCAA service has to compete for system resources, the BCAA response to the authentication request could take longer.

## Step Four: Verify Disk Space

See "BCAA Disk Space Requirements" on page 7.

## Step Five: Check BCAA Support and Installation Requirements

BCAA 6.1 introduces changes in BCAA installation. All previous BCAA installations must be deleted before installing BCAA 6.1. The uninstall process retains the .ini files from previous BCAA 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 BCAA 6.1. If the release requires a different BCAA version, you must uninstall BCAA 6.1 and install the BCAA 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 BCAA 6.1 and install the required BCAA 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

To install or upgrade BCAA, the service has to be stopped while files are copied during the installation process. If you have configured an alternate BCAA server, the ProxySG appliance will fail over to that server when BCAA is stopped. If you have not configured an alternate BCAA 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 BCAA, make sure that you have at least 45 MB of disk space on your Windows server. Although some versions of BCAA might require less than 45 MB of disk space, allocating 45 MB of disk space will address the needs to complete the BCAA 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

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 6.1 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

## IWA

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

- The BCAA 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 BCAA service must share a secret with a Kerberos server (called a KDC) and register an appropriate Service Principal Name (SPN).

## Windows SSO

The BCAA service is used to supply mappings for IP addresses to logged on users. The Windows 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 BCAA 6.1.

## Novell SSO

The BCAA service manages communication with the Novell eDirectory server.

## SiteMinder

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

Before you can use the BCAA 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.



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

---



# 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, please 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 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	✓			



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 BCAA

The following procedure describes how to install BCAA 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 BCAA

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

The first time you download files, you are prompted to install the Download Manager. Follow the onscreen prompts to download and run the installer. For more information, refer to <https://www.symantec.com/support-center/getting-started>.

## Step Three: Install BCAA

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

If you try to install BCAA version 6.1 before removing the previous version, you will receive an error. For help, see "Help with Uninstalling Previous BCAA Versions" on page 11.
2. Unzip the BCAA Setup file and double-click the .exe file to launch the BCAA Setup.
3. To begin the setup, click **Next**.
4. Specify a destination folder for the BCAA software.

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



If you are installing on a system that had a previous BCAA 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 BCAA and the ProxySG appliance will use to communicate.

By default, both BCAA 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 you would like it to be opened. You must also make sure that this port is not blocked, for example by another firewall between the BCAA 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 BCAA:

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

The SSL settings on the ProxySG appliance and BCAA 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 BCAA; 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 BCAA 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 BCAA and the ProxySG, select **Yes**. Otherwise, select **No**.

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

8. Indicate whether the BCAA installation will support a ProxySG appliance using a Windows SSO realm or a PacketShaper.
  - Select **No** if you are using BCAA with Novell SSO, SiteMinder, IWA/Basic, IWA/NTLM.
  - Select **Yes** if:
    - You are using BCAA with Windows SSO or a PacketShaper.
    - You are using BCAA with Windows 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\bcaa\_user or bcaa\_user@mydomain.com).

9. If you selected **No** in Step 8, you must now specify whether to run BCAA as the LocalSystem account or as a domain user. If you are using BCAA 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 BCAA dialog.

## Uninstalling or Modifying the BCAA 6.1 Service

To modify the BCAA installation, uninstall and reinstall.

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.



For help with uninstalling previous BCAA versions, refer to KB5915 *Cannot uninstall old version of BCAA as it is missing from Add/Remove Programs*.

---

# Troubleshoot BCAAA

The following topics describe common BCAAA problems and solutions.

- "Troubleshoot Authentication Agent Problems" on page 17
- "Troubleshoot SSL Support" on page 16
- "Determine the BCAAA Version" on page 18
- "View or Modify BCAAA Service Properties" on page 15
- "Common BCAAA Event Messages" on page 19

# 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 19.

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 BCAA 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 BCAA connection.

**Solution:** Enable TLSv1 on the default SSL device profile.



- 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.



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

---

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

**Solution:** Give the BCAA user access to the certificate store.

Stop the BCAA service. From the Run prompt, launch the regedit program to give the BCAA 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 19.

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 BCAA Version

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

## Control Panel

Complete the following steps:

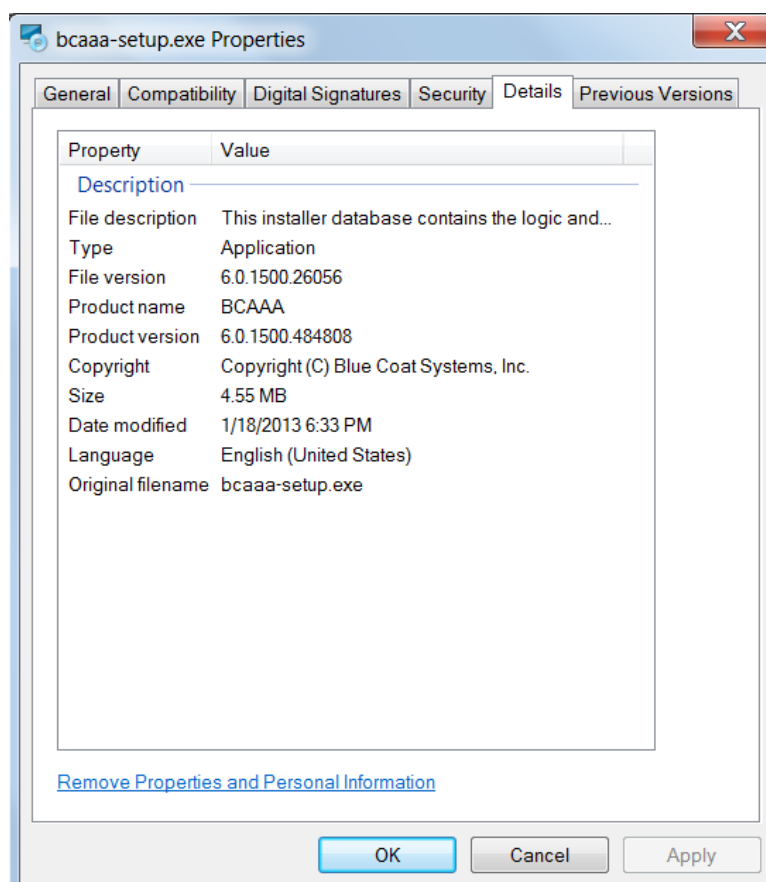
1. Click **Start > Control Panel**.
2. Click **Programs and Features**.
3. After the list populates, find BCAA and read the version number listed in the **Version** column.

## 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 BCAA Event Messages

The following table describes the common BCAA 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 BCAA.

## View the application event log

To view the BCAA event log:

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

For each BCAA 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.
1008	ConnectNamedPipe failed, pipe='%s'	The agent process could not obtain the information from the dispatcher on the named pipe for the reason given.

Message ID	Message	Description
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 BCAA server does not have the same version of BCAA 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\lx'	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.

Message ID	Message	Description
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.
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-of-interest: 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.

Message ID	Message	Description
1225	Error calling Look-upPrivilegeValue	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.
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.

Message ID	Message	Description
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.
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.

Message ID	Message	Description
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.
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.



Message ID	Message	Description
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.
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 BCAA 6.1

BCAA 6.1 introduces the following changes:

- BCAA v6.0 does not support the COREid realm.
- A Solaris version of BCAA is no longer provided.
- You must uninstall the previous BCAA installation before installing version 6.1. If you try to install BCAA 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 BCAA installation, uninstall and reinstall.
- BCAA event log messages now refer to a generic device name (for example, remote appliance) instead of ProxySG.
- BCAA no longer requires “Act as part of the operating system” privilege for IWA realms.

### Changes in 6.1.2

---

- First release: September 2013.
- BCAA 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 BCAA. (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 BCAA stopped authenticating requests and became unresponsive when a high number of BCAA realm processes were created after a network device corrupted the initial data from the proxy to BCAA. (B#254189)
- IPv6 is now supported for connecting to BCAA for proxies running SG 6.7.4 or later.

## Additional References

Refer to the following documents for additional information. Additionally, there are a number of articles at MySymantec (<https://support.symantec.com>).

- *IWA Authentication - Fundamentals and Deployment Guidelines:*

<http://www.symantec.com/docs/DOC9827>

- *How to Implement Proxy Authentication:*

<http://www.symantec.com/docs/TECH242110>

- *What Ports Does BCAAA Use?*

<http://www.symantec.com/docs/TECH243202>

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

<http://www.symantec.com/docs/TECH241635>

# Copyrights

Copyright © 2017 Symantec Corp. All rights reserved. Symantec, the Symantec Logo, the Checkmark Logo, Blue Coat, and the Blue Coat logo are trademarks or registered trademarks of Symantec Corp. or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE. SYMANTEC CORPORATION PRODUCTS, TECHNICAL SERVICES, AND ANY OTHER TECHNICAL DATA REFERENCED IN THIS DOCUMENT ARE SUBJECT TO U.S. EXPORT CONTROL AND SANCTIONS LAWS, REGULATIONS AND REQUIREMENTS, AND MAY BE SUBJECT TO EXPORT OR IMPORT REGULATIONS IN OTHER COUNTRIES. YOU AGREE TO COMPLY STRICTLY WITH THESE LAWS, REGULATIONS AND REQUIREMENTS, AND ACKNOWLEDGE THAT YOU HAVE THE RESPONSIBILITY TO OBTAIN ANY LICENSES, PERMITS OR OTHER APPROVALS THAT MAY BE REQUIRED IN ORDER TO EXPORT, RE-EXPORT, TRANSFER IN COUNTRY OR IMPORT AFTER DELIVERY TO YOU.

## Americas:

Symantec Corporation

350 Ellis Street

Mountain View, CA 94043

## Rest of the World:

Symantec Limited

350 Ellis Street Ballycoolin Business Park

Blanchardstown, Dublin 15, Ireland