Monitoring Citrix App Controller

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

Citrix App Controller delivers access to web, SaaS, Android, and iOS apps, as well as integrated ShareFile data and documents. Users access their applications through Citrix Receiver, Receiver for Web or Worx Home.

With App Controller, you can provide the following benefits for each application type:

- **SaaS applications.** Active Directory-based user identity creation and management, with SAML-based single sign-on (SSO).
- **Intranet web applications.** HTTP form-based SSO by using password storage.
- **iOS and Android apps.** Unified store to which you can install MDX apps for iOS and Android devices, and security management for MDX policies, encompassing WorxMail and WorxWeb. You can wrap iOS and Android apps with the MDX Toolkit to create MDX apps.
- **ShareFile access.** Delivery of files by configuring ShareFile settings and the ShareFile application that provides seamless SAML SSO, and Active Directory-based ShareFile service user account management.

Any issue that threatens the availability or overall health of the App Controller will impact user access to all the aforesaid applications. For instance, if the network connection to the App Controller is flaky or broken, users will not be able to access SaaS, mobile applications, or ShareFile; as a result, user productivity will suffer. Similarly, the inaccessibility of App Controller's web-based management console and the use of expired certificates to establish a connection with a mobile app can also slowdown/suspend user access. What can further weaken a user's experience with a mobile app are the application-level policies and device-level securities configured on App Controller for the individual applications.

Therefore, to assure mobile device users of a high-quality experience with their applications, administrators should closely monitor the availability of the App Controller, track user logins to App Controller and the applications these users typically access, study the current policy settings for applications, and proactively detect abnormalities and areas that require fine-tuning. This is exactly where the Citrix App Controller monitoring model that eG Enterprise provides help!

Chapter 2: How to Monitor Citrix App Controller Using eG Enterprise?

eG Enterprise capable of monitoring the Citrix App Controller in an agentless manner. All that is required for this is a single eG agent on any remote Windows host in the environment. The below two mechanisms are used by the eG enterprise to pull out performance statistics related to the health and operations of the Citrix App Controller.

- The eG tests connect to Citrix App Controller's management console to pull out wide range of metrics and/or;
- The eG tests parse a Syslog created on the Syslog server that hosts the Syslog server used by the Citrix App Controller for collecting metrics.

To enable the eG agent to use the aforesaid mechanisms, a set of pre-requisites should be fulfilled. These requirements have been discussed in the below section.

2.1 Pre-requisites for monitoring Citrix App Controller

To enable the eG agent to collect performance metrics from the App Controller, the following pre-requisites should be fulfilled:

- The eG agent should be deployed on the Syslog server that hosts the Syslog file used for metrics collection.
- The eG agent has to be configured with the credentials of a user to App Controller. The user should be vested with *Administrator* privileges.

Once the above-said pre-requisites are fulfilled, proceed to manage the Citrix App Controller component for monitoring. The procedure for achieving this has been explained in the below section.

2.2 Managing the Citrix App Controller

The Citrix App Controller cannot be automatically discovered by eG Enterprise. This implies that you will have to manually add the Citrix AppController into the eG Enterprise system to manage it. Follow the steps below to achieve the same:

1. Login to the eG administrative interface.
2. Follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu.
3. In the **COMPONENTS** page that appears, select *Citrix AppController* from the **Component type** drop-down and then click the **Add New Component** button.

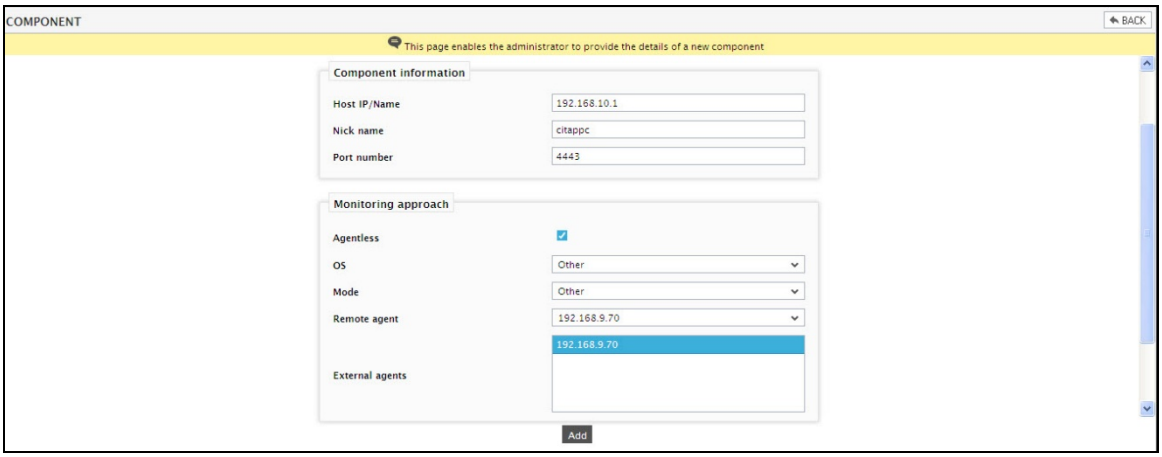

Figure 2.1: Adding a Citrix AppController server

4. Specify the **Host IP/Name** and the **Nick name** of the App Controller in 2.2. Since the App Controller is monitored in an agentless manner, select **Other** as the **OS** and **Other** as the **Mode**.
5. The **Port number** will be set as 4443 by default. If the App Controller is listening on a different port in your environment, then override this default setting.
6. Then, click the **Add** button to add the App Controller for monitoring.

2.3 Configuring the tests

1. When you attempt to sign out, a list of unconfigured tests will appear as shown in Figure 2.2.

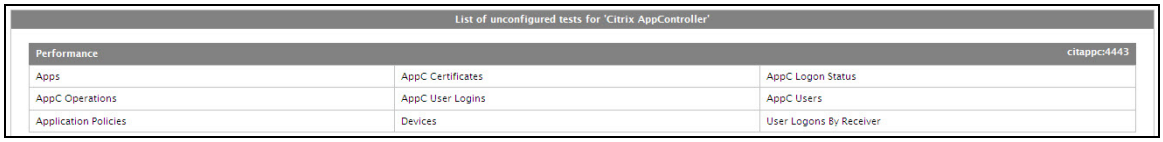

Figure 2.2: List of unconfigured tests to be configured for the Citrix App Controller

2. Click on the tests to configure them. To know how to configure these tests, refer to **Monitoring**

Citrix App Controller chapter.

3. Finally, signout of the eG administrative interface.

Chapter 3: Monitoring Citrix App Controller

eG Enterprise Suite provides specialized monitor for the Citrix App Controller. This out-of-the-box monitor periodically checks and reports the availability, responsiveness, and overall health of each of the App Controller.

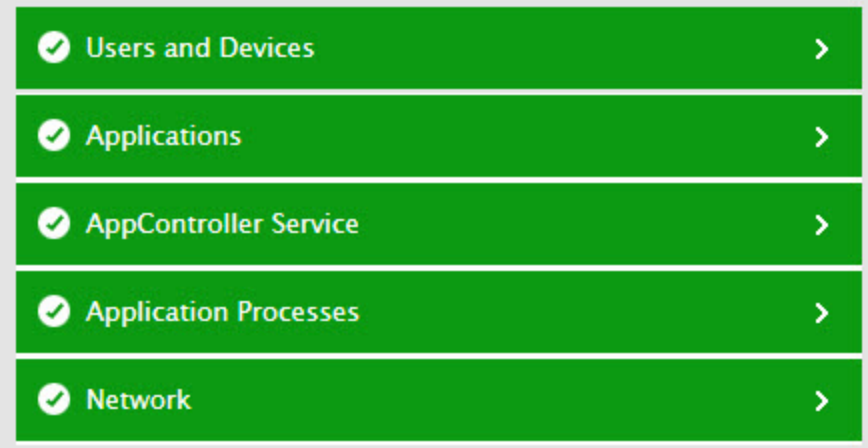

Figure 3.1: The layer model of a Citrix App Controller

Each layer of this model is mapped to tests to collect performance metrics of the App Controller. Using the metrics so collected, administrators can ascertain the following:

- Is the App Controller management console accessible? If so, how quickly are users able to connect to the console?
- Is any SSL certificate installed on the App Controller nearing expiry? If so, which one is it?
- Are there any issues logging into App Controller?
- What is the current session load on the App Controller? Which devices are currently connected to the App Controller?
- Which are the popular applications on the App Controller, on the basis of the number of launches? Which is the receiver that is used most often for accessing applications on the App Controller?
- Have any applications been configured to not run on jail broken or rooted devices? Which applications are these?
- Which applications block the use of the camera, microphone, and SMS composition?

The sections that follow will take you on a layer-by-layer tour of the Citrix App Controller monitoring model. However, since the tests associated with the **Network** layer have been already dealt with in detail in the *Monitoring Unix and Windows Servers* document this chapter will focus on the other layers only.

3.1 The AppController Service Layer

The tests mapped to this layer tracks the validity of all active certificates, the details on the users logging into AppController and the operations that performed on the AppController by the users.

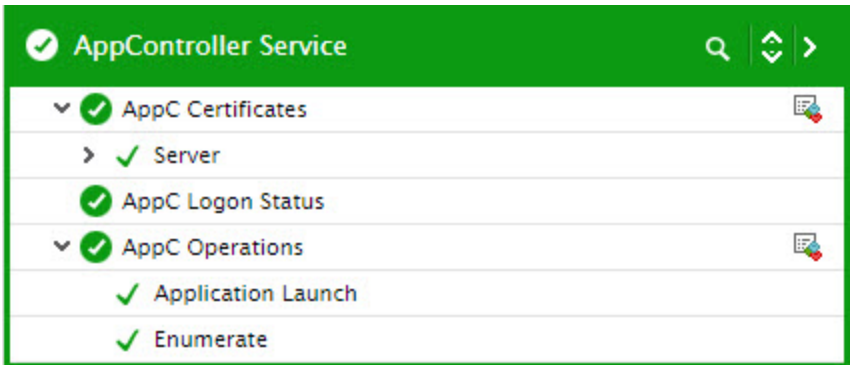

Figure 3.2: The tests mapped to the AppController Service layer

3.1.1 AppC Certificates Test

In App Controller, certificates are used to create secure connections and authenticate users.

To establish a secure connection, a server certificate is required at one end of the connection. A root certificate of the Certificate Authority (CA) that issued the server certificate is required at the other end.

- **Server certificate**. A server certificate certifies the identity of a server. App Controller requires this type of digital certificate.
- **Root certificate.** A root certificate identifies the CA that signed the server certificate. The root certificate belongs to the CA. The user device requires this type of digital certificate to verify the server certificate.

You can configure certificate chains, which contain intermediate certificates, between the server certificate and the root certificate. Both root certificates and intermediate certificates are referred to as trusted certificates.

App Controller requires root and server certificates to communicate in the following ways:

- Between App Controller and the App Controller management console
- Between applications and App Controller
- Between App Controller and StoreFront

If an active certificate (be it a server, root, or an intermediate certificate) suddenly expires, applications will no longer be able to communicate with App Controller and vice-versa. To avoid this, administrators should proactively identify certificates nearing expiry and renew the certificates. This is where the **AppC Certificates** test helps. This test captures the expiry date of all active certificates, computes how long each active certificate will remain valid, and proactively alerts administrators if any certificate is nearing expiry.

Target of the test : Citrix App Controller

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every active SSL certificate installed on the App Controller.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which the test is being configured.
Port	The port at which the host listens. By default, this is *NULL*.
Report Only Active Certificates	By default, this flag is set to **Yes**, indicating that this test reports the validity of active certificates only. To ensure that the test reports the validity of all certificates, set this flag to **No**.
Username and Password	To pull out metrics, this test needs to login to the AppController's management console as a user with *Administrator* rights to AppController. For this purpose, you need to configure this test with the Username and Password of a user with *Administrator* rights to the AppController.
Confirm Password	Confirm the Password by retyping it here.
SSL	Indicate whether/not AppController is SSL-enabled. By default, this flag is set to **Yes**.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are

Parameter	Description
	detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Status	Indicates the current status of this SSL certificate.		The values that this measure reports and their corresponding numeric values are listed in the table below: **Measure Value** / **Numeric Value** Active / 1 Expired / 0 **Note:** By default, this measure reports the **Measure Value**s discussed in the table above. However, in the graph of this measure, the status of the certificate is indicated using the numeric equivalents only.
Valid upto	Indicates how long this certificate will remain valid.	Days	A high value is desired for this measure. A very low value indicates that the certificate is about to expire very soon. You may want to consider renewing the certificate before this eventuality strikes. Use the detailed diagnosis of this measure to know the exact date on which the certificate will expire.

3.1.2 AppC Logon Status Test

Frequent login failures and inexplicable delays when accessing the AppController can have an adverse impact on a user's experience with AppController. To capture such failures/delays proactively and isolate their root-cause, administrators can use the **AppC Logon Status** test. At configured intervals, this test emulates a user logging into AppController. In the process, the test captures every step of the user login and reports the time taken at each step. This way, unusual slowness in logging in can be captured and where the login process was delayed can be determined – when connecting to the AppController? Or when authenticating?

Target of the test : Citrix AppController

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the Citrix AppController being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which the test is being configured.
Port	The port at which the host listens. By default, this is *NULL*.
Username and Password	To pull out metrics, this test needs to login to the AppController's management console as a user with *Administrator* rights to AppController. For this purpose, you need to configure this test with the Username and Password of a user with *Administrator* rights to the AppController.
Confirm Password	Confirm the Password by retyping it here.
SSL	Indicate whether/not AppController is SSL-enabled. By default, this flag is set to **Yes**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Connection status	Indicates whether/not the user could connect to the AppController.		The values that this measure reports and their corresponding numeric values are listed in the table below:

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Success</td><td>1</td></tr>
<tr><td>Failed</td><td>0</td></tr>
</table>
Note:
By default, this measure reports the Measure Values discussed in the table above. However, in the graph of this measure, the status of the connection is indicated using the numeric equivalents only.
</td></tr>
<tr><td>Time taken to connect</td><td>Indicates the time taken to connect to the AppController.</td><td>Secs</td><td>A low value is desired for this measure. A high value indicates a connection bottleneck.</td></tr>
<tr><td>Authentication status</td><td>Indicates whether/not the login credentials of the user were successfully authenticated.</td><td></td><td>The values that this measure reports and their corresponding numeric values are listed in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Success</td><td>1</td></tr>
<tr><td>Failed</td><td>0</td></tr>
</table>
Note:
By default, this measure reports the Measure Values discussed in the table above. However, in the graph of this measure, the status of the authentication is indicated using the numeric equivalents only.</td></tr>
<tr><td>Time taken to authenticate</td><td>Indicates the time taken to authenticate the user login.</td><td>Secs</td><td>A high value for this measure could indicate an authentication delay.</td></tr>
<tr><td>Time taken to login</td><td>Indicates the total time taken to login.</td><td>Secs</td><td>A high value indicates a login delay. In this case, you can compare the value of the Time taken to connect and</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			Time taken to authenticate measures to know where the login was bottlenecked.

3.1.3 AppC Operations Test

If a user complains that his/her transactions with the App Controller are failing, administrators may first want to know which steps of the user interactions are failing often. The **AppC Operations** test provides administrators with this useful information. This test scans the AppController Syslog file for the type of operations users performed on AppController. For every operation so discovered, this test then reports the number of times that operation succeeded and the number of times it failed. This way, the test highlights those operations that failed very often and caused the user experience with the AppController to suffer.

For this test to run and report metrics, the AppController should be configured to create a Syslog file in a remote Syslog server, where the details and status of all user interactions with the AppController will be logged. The steps for achieving the same are discussed in the below section.

3.1.3.1 Configuring the Syslog server

To configure the Syslog server where this Syslog file should be created, do the following:

1. Connect to the AppController management console using the URL: https://<IP_address_of_AppController>:<AppController_port>
2. Login to the AppController as an *administrator*.
3. Figure 3.3 will then appear. Click the **Settings** option in Figure 3.3.

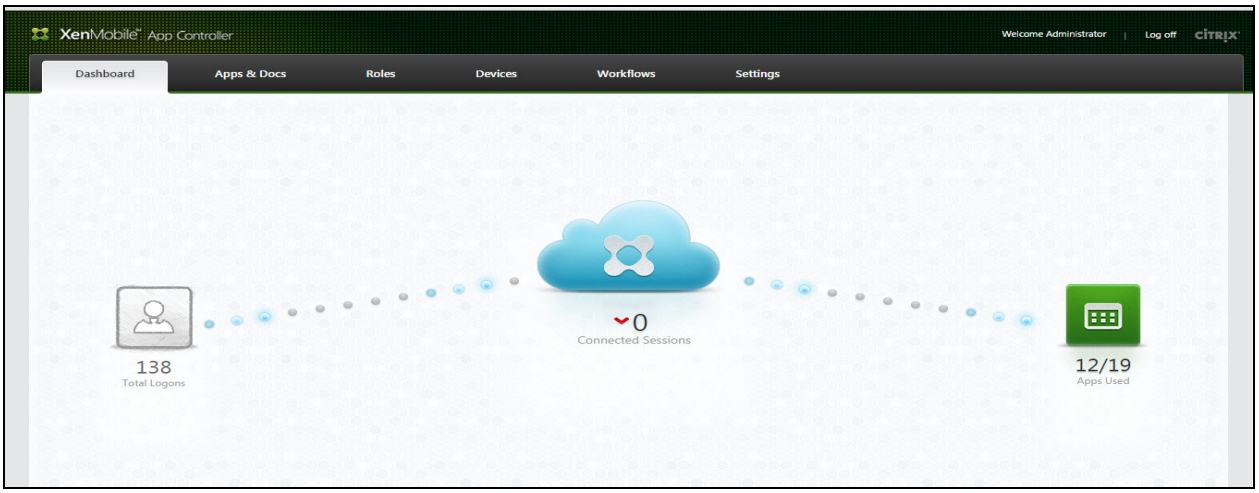

Figure 3.3: The AppController management console

4. Next, scroll down the **System Configuration** panel of Figure 3.4 until the **Syslog** option becomes visible. Then, click the **Syslog** option. This will bring up a **Syslog** page in the right panel, where you can configure a remote Syslog server and enable Syslog file creation on the server.

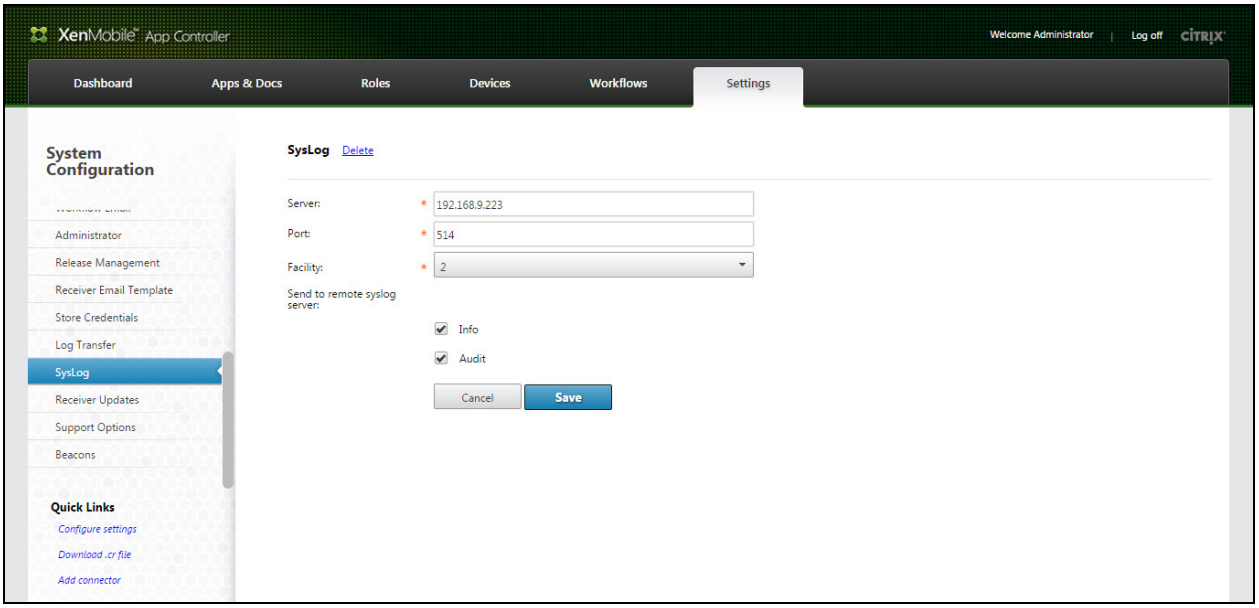

Figure 3.4: Configuring the Syslog server where the Syslog file is to be created

5. To configure a new Syslog server, enter the IP address of the Syslog server in the **Server** text box of Figure 3.4.
6. Enter the **Port** at which the Syslog server listens.
7. Let the **Facility** remain at 2.

8. Then, indicate what details should be logged in the Syslog file that will be created in the specified Syslog server. For the eG tests to work, at least the **Audit** check box should be selected.
9. Click the **Save** button in Figure 3.4 to register the changes.

Target of the test : Citrix AppController

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every operation users performed on the AppController.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which the test is being configured.
Port	The port at which the host listens. By default, this is *NULL*.
Log File Path	This test reports metrics by parsing a Syslog file. Specify the full path to the Syslog file here. To know how to configure the Syslog server where the AppController will be creating this file, refer to Section **3.1.3.1**.
SSL	Indicate whether/not AppController is SSL-enabled. By default, this flag is set to **Yes**.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Successful	Indicates the number of	Number	A high value is desired for this

Measurement	Description	Measurement Unit	Interpretation
operations	times this operation succeeded.		measure. Use the detailed diagnosis of this measure to view the names of the users who succeeded in performing an operation, when they performed the operation, and the client/receiver each user used for this purpose.
Failed operations	Indicates the number of times this operation failed.	Number	A very low value is desired for this measure. Use the detailed diagnosis of this measure to view the names of the users who failed to perform a particular operation, when they tried to perform that operation, and the client/receiver each user used for this purpose.

The detailed diagnosis of the *Successful operations* measure reveals the names of the users who succeeded in performing an operation, when they performed the operation, and the client/receiver each user used for this purpose.

Figure 3.5: The detailed diagnosis of the Successful operations measure

3.2 The Applications Layer

Using the tests mapped to this layer, application launches can be audited and the effectiveness of application policies can be measured.

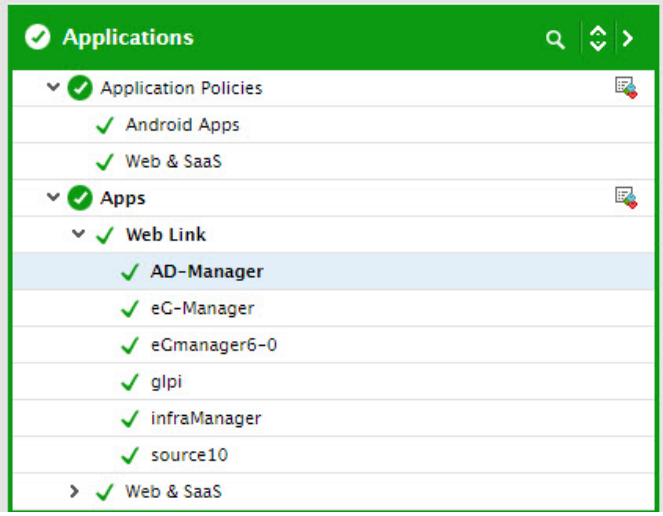

Figure 3.6: The tests mapped to the Applications layer

3.2.1 Application Policies Test

You can set policies for mobile apps in the App Controller management console. Application policies for Android or iOS apps fall into the following three main categories:

- **Information security**. These policies are designed to protect app data and documents. The policies dictate how information can be exchanged between apps. You can configure settings for the app to allow or prevent user access to such operations as printing, email, text messaging, and use of the device camera.
- **Application access**. These policies determine the logon requirements users must meet in order to open an app. You can configure authentication methods, settings to prevent apps from running on a jailbroken, or rooted, device, network connection requirements, and conditions for locking or erasing app data.
- **Network**. These policies determine the network settings for traffic to and from the app. You can configure the following settings: allow unrestricted access to the internal network, redirect traffic through XenMobile App Edition by using a VPN tunnel specific to each app, or block all traffic from accessing the internal network.

Application policies for Web & SaaS apps on the other hand, fall into the following categories:

- **Device security:** This policy prevents jail broken or rooted devices from accessing apps.
- **Network:** These policies determine the network settings for communicating with the app.

Periodically, administrators will have to review these policies, identify the applications on which these policies have been configured, and decide whether the restrictions imposed by the policies on

the applications should continue, should be made stronger, or can be lifted. The **Application Policies** test helps administrators in this exercise. For each category of applications delivered by the AppController, this test reports the number of applications (of that type/category) on which certain key usage policies have been enforced. Detailed metrics collected by this test also reveal the names of these applications. Using this information, administrators can quickly identify where policy changes may have to be effected.

Target of the test : Citrix AppController

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each category of applications delivered by the Citrix AppController being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which the test is being configured.
Port	The port at which the host listens. By default, this is *NULL*.
Username and Password	To pull out metrics, this test needs to login to the AppController's management console as a user with *Administrator* rights to AppController. For this purpose, you need to configure this test with the Username and Password of a user with *Administrator* rights to the AppController.
Confirm Password	Confirm the Password by retyping it here.
SSL	Indicate whether/not AppController is SSL-enabled. By default, this flag is set to **Yes**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Application blocking jailbroken or rooted devices	Indicates the number of applications of this type that have been configured to not run on jailbroken or rooted devices.	Number	Use the detailed diagnosis of this measure to identify those applications that will not run on jailbroken or rooted devices.
Device pin or	Indicates the number of	Number	Use the detailed diagnosis of this measure

Measurement	Description	Measurement Unit	Interpretation
password required applications	applications of this type that can be accessed only when a device pin or a password is provided.		to identify those applications that support password- or pin-protected access.
Camera blocking applications	Indicates the number of applications of this type that prevent the use of the camera.	Number	Use the detailed diagnosis of this measure to identify those applications that block camera usage.
Microphone blocking applications	Indicates the number of applications of this type that do not allow the use of a microphone.	Number	Use the detailed diagnosis of this measure to identify those applications that disallow microphone usage.
Location services blocking applications	Indicates the count of applications of this type that prevent the use of location services (eg., GPS or network).	Number	Use the detailed diagnosis of this measure to know which applications prevent the use of location services.
“SMS Compose” blocking applications	Indicates the number of applications of this type that block SMS (compose).	Number	Use the detailed diagnosis of this measure to know which applications block SMS.
“Screen Capture” blocking applications	Indicates the number of applications of this type that prevent a user-initiated screen capture when running.	Number	Use the detailed diagnosis of this measure to know which applications block screen capture operations.
Device sensors blocking applications	Indicates the number of applications of this type that do not permit the use of device sensors, like accelerometer, motion sensor, or gyroscope.	Number	Use the detailed diagnosis of this measure to know which applications do not allow the use of device sensors.
Application logs blocking applications	Indicates the number of applications of this type that block application	Number	Use the detailed diagnosis of this measure to know which applications do not allow the logging of application events.

Measurement	Description	Measurement Unit	Interpretation
	logs.		
Full VPN tunnel enabled applications	Indicates the number of applications of this type that use an application-specific VPN tunnel through Netscaler Gateway for accessing the internal network.	Number	Use the detailed diagnosis of this measure to know which applications use a VPN tunnel to access the internal network.
“Access limits for public files” applications	Indicates the number of applications of this type that have been configured with ‘Access limits for public files’.	Number	In the App Controller management console, administrators can set the Access limits for public files policy for an application. This contains a comma-separated list. Each entry is a regular expression path followed by (NA), (RO), or (RW). Files matching the path are limited to No Access, Read Only, or Read Write access. The list is processed in order and the first matching path is used to set the access limit. This policy is enforced only when the Public file encryption policy is enabled (changed from the Disable option to the SecurityGroup or Application option). This policy is applicable only to existing, unencrypted public files and specifies when these files are encrypted. Use the detailed diagnosis of this measure to know for which applications access limits have been configured for public files.
Wifi require applications	Indicates the number of applications of this type that have been set to run only when the device is connected to a Wifi network.	Number	Use the detailed diagnosis of this measure to know which applications require a Wifi connection for execution.
“Network access” blocking applications	Indicates the number of applications of this type that have block all	Number	Use the detailed diagnosis of this measure to know which applications block network access for the devices they run on.

Measurement	Description	Measurement Unit	Interpretation
	network access for the device they run on.		

3.2.2 Apps Test

This test auto-discovers the applications configured on the AppController and reports the number of successful and failed launches per application.

For this test to run and report metrics, the AppController should be configured to create a Syslog file in a remote Syslog server, where the details and status of all user interactions with the AppController will be logged. To know how to configure the Syslog server where the AppController will be creating this file, Section **3.1.3.1**.

Target of the test : Citrix AppController

Agent deploying the test : A remote agent

Outputs of the test : One set of results each application configured on the Citrix AppController being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which the test is being configured.
Port	The port at which the host listens. By default, this is *NULL*.
Log File Path	This test reports metrics by parsing a Syslog file. Specify the full path to the Syslog file here. To know how to configure the Syslog server where the AppController will be creating this file, Section **3.1.3.1**.
Username and Password	To pull out metrics, this test needs to login to the AppController's management console as a user with *Administrator* rights to AppController. For this purpose, you need to configure this test with the Username and Password of a user with *Administrator* rights to the AppController.
SSL	Indicate whether/not AppController is SSL-enabled. By default, this flag is set to **Yes**.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an

Parameter	Description
	optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Number of successful application launches	Indicates the number of times this application was launched successfully during the last measurement period.	Number	Use the detailed diagnosis of this measure to view the names of the users who successfully launched the application, when they launched, and the client/receiver each user used.
Number of failed application launches	Indicates the number of times this application was launched unsuccessfully during the last measurement period.	Number	Compare the value of this measure acros applications to know which application failed very often. Use the detailed diagnosis of this measure to view the names of the users for whom application launches failed, when they attempted to launch, and the client/receiver that was used for the attempt.

3.3 The User and Devices Layer

The tests mapped to this layer track user logins to the AppController, measures the logon duration per user, and pinpoints the root-cause of logon slowness. In addition, this layer also keeps an eye on the devices connected to the AppController, and points to those devices that have been locked/erased.

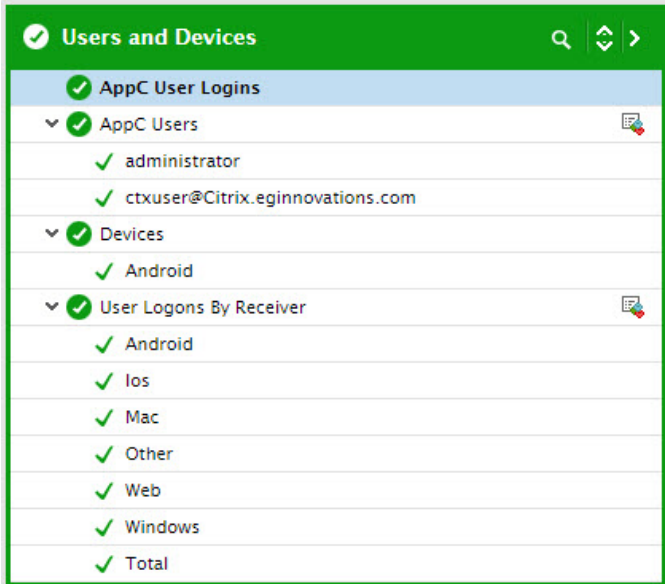

Figure 3.7: The tests mapped to the User and Devices layer

3.3.1 AppC User Logins Test

By tracking user sessions to the AppController, the **AppC User Logins** test helps administrators gauge the workload of the App Controller and quickly capture failed login attempts.

For this test to run and report metrics, the App Controller should be configured to create a Syslog file in a remote Syslog server, where the details and status of all user interactions with the App Controller will be logged. To know how to configure the Syslog server where the App Controller will be creating this file, Section **3.1.3.1**.

Target of the test : Citrix App Controller

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the Citrix App Controller being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which the test is being configured.
Port	The port at which the host listens. By default, this is *NULL*.
Log File Path	This test reports metrics by parsing a Syslog file. Specify the full path to the Syslog file

Parameter	Description
	here. To know how to configure the Syslog server where the AppController will be creating this file, Section **3.1.3.1**.
SSL	Indicate whether/not AppController is SSL-enabled. By default, this flag is set to **Yes**.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Connected sessions	Indicates the total number of users currently connected to the AppController.	Number	This is a good indicator of the current session load on the AppController.
New logins	Indicates the number of users who logged in during the last measurement period.	Number	
Percentage of new logins	Indicates the percentage of users who logged in recently.	Percent	
Session logouts	Indicates the number of sessions that logged out during the last measurement period.	Number	A sudden increase in the value of this measure could warrant closer scrutiny.
Failed logins	Indicates the number of logins that failed.	Number	A low value is desired for this measure.

3.3.2 AppC Users Test

To assess a user's experience with the AppController, administrators must track a user's sessions on the AppController and audit the quality of the application launches attempted by that user. The **AppC Users** test does exactly this! This test auto-discovers the users who are currently logged into the AppController, and for each user, reports the open sessions for that user and the number of successful and failed application launches per user. This way, the test points to those users with the maximum number of failed application launches. Such users naturally are the ones with a poor quality experience with the AppController.

For this test to run and report metrics, the AppController should be configured to create a Syslog file in a remote Syslog server, where the details and status of all user interactions with the AppController will be logged. To know how to configure the Syslog server where the AppController will be creating this file, Section **3.1.3.1**.

Target of the test : Citrix AppController

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the Citrix AppController being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which the test is being configured.
Port	The port at which the host listens. By default, this is *NULL*.
Log File Path	This test reports metrics by parsing a Syslog file. Specify the full path to the Syslog file here. To know how to configure the Syslog server where the AppController will be creating this file, Section **3.1.3.1**.
Show Other Users	The test discovers the users who are currently logged into the AppController by reading the entries in the **User** column of the specified syslog file. Sometimes, this column may have a few blank entries. By default, this test ignores these blank entries. This is why, the Show Other Users flag is set to **No** by default. If you set this flag to **Yes**, then the test will report metrics for these blank entries as well. In this case, the test will additionally report a set of metrics for an **Others** descriptor. Each measure of the Others descriptor will report a value that is an aggregate of the values recorded for the blank entries in the Syslog file.

Parameter	Description
SSL	Indicate whether/not AppController is SSL-enabled. By default, this flag is set to **Yes**.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
User sessions	Indicates the number of open sessions for this user currently.	Number	This is a good indicator of the session load imposed by a particular user on the AppController. In the event of a session overload, you can compare the value of this measure across users to know which user has contributed to the overload. Use the detailed diagnosis of this measure to know which applications are being accessed by a user and which client/receiver that user is using to launch the application.
Successful application launches	Indicates the number of successful application launches for this user.	Number	Use the detailed diagnosis of this measure to know which applications were successfully launched by a user and which client/receiver that user used to launch each application.
Failed application launches	Indicates the number of application launches that failed for this user.	Percent	Use the detailed diagnosis of this measure to know which applications a user could not launch and which

Measurement	Description	Measurement Unit	Interpretation
			client/receiver that user used to launch each application.

3.3.3 Devices Test

Tracking the devices connected to the AppController will not only indicate the current device load on the AppController, but will also shed light on the current device status. Based on this status information, administrators can determine whether/not device status needs to be changed. This is exactly what the **Devices** test enables administrators to perform. This test reports the number of devices currently connected to AppController and also reveals the number and names of the connected devices that are locked and/or erased. If a user complains that he/she is unable to access some applications, then administrators can use this information to quickly determine whether the user device is indeed 'authorized' to access the applications or have been locked out or erased. Using the same information, administrators can also determine whether the user device is now 'safe' for use and can hence be unlocked or need not be erased.

Target of the test : Citrix AppController

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the Citrix AppController being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which the test is being configured.
Port	The port at which the host listens. By default, this is *NULL*.
Username and Password	To pull out metrics, this test needs to login to the AppController's management console as a user with *Administrator* rights to AppController. For this purpose, you need to configure this test with the Username and Password of a user with *Administrator* rights to the AppController.
Confirm Password	Confirm the Password by retyping it here.
SSL	Indicate whether/not AppController is SSL-enabled. By default, this flag is set to **Yes**.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an

Parameter	Description
	optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total devices	Indicates the total number of devices currently connected to the AppController.	Number	This is a good indicator of the current device load on the AppController.
Locked devices	Indicates the number of devices connected to AppController that are locked.	Number	If users lose an iOS or Android device, you can lock applications on the device that App Controller delivers, which prevents unauthorized access to the applications. Once the device is found, you can unlock the applications on that device. Use the detailed diagnosis of this measure to identify the devices on which applications have been locked.
Erased devices	Indicates the number of devices connected to AppController that have been erased.	Number	If users lose an iOS or Android device and do not locate the device in a specified period of time, or if the user leaves the organization, you can erase application data and ShareFile documents from the user device. If you determine that the device is safe, you can stop erasing the data and

Measurement	Description	Measurement Unit	Interpretation
			documents on the device. Use the detailed diagnosis of this measure to identify the devices on which application data and ShareFile documents have been erased.

3.3.4 User Logons by Receiver Test

To know which receiver is used by most of the users connecting to AppController, take the help of the **User Logons by Receiver** test. For every receiver connecting to the AppController, this test reports the total number of users currently logged in via that receiver; a quick comparison of user logons across receivers will point you to the most popular receiver.

Target of the test : Citrix AppController

Agent deploying the test : A remote agent

Outputs of the test : One set of results each receiver connecting to the AppController.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which the test is being configured.
Port	The port at which the host listens. By default, this is *NULL*.
Username and Password	To pull out metrics, this test needs to login to the AppController's management console as a user with *Administrator* rights to AppController. For this purpose, you need to configure this test with the Username and Password of a user with *Administrator* rights to the AppController.
Confirm Password	Confirm the Password by retyping it here.
SSL	Indicate whether/not AppController is SSL-enabled. By default, this flag is set to **Yes**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Number of users currently on	Indicates the number of users currently logged into AppController via this receiver.	Number	Compare the value of this measure across receivers to know which receiver was used by most of the users logged in currently.
Local users	Indicates the number of users from the internal network who logged into AppController via this receiver.	Number	
External users	Indicates the number of users who used this receiver to log into AppController from outside the internal network (for example, users who connect from the Internet or from remote locations).	Number	

About eG Innovations

eG Innovations provides intelligent performance management solutions that automate and dramatically accelerate the discovery, diagnosis, and resolution of IT performance issues in on-premises, cloud and hybrid environments. Where traditional monitoring tools often fail to provide insight into the performance drivers of business services and user experience, eG Innovations provides total performance visibility across every layer and every tier of the IT infrastructure that supports the business service chain. From desktops to applications, from servers to network and storage, from virtualization to cloud, eG Innovations helps companies proactively discover, instantly diagnose, and rapidly resolve even the most challenging performance and user experience issues.

eG Innovations is dedicated to helping businesses across the globe transform IT service delivery into a competitive advantage and a center for productivity, growth and profit. Many of the world's largest businesses use eG Enterprise to enhance IT service performance, increase operational efficiency, ensure IT effectiveness and deliver on the ROI promise of transformational IT investments across physical, virtual and cloud environments.

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

To contact eG Innovations sales team, email sales@eginnovations.com.