

AppExchange Certification Welcome Kit

Table of Contents

1	Introduction.....	2
2	Why Certify?	2
3	AppExchange Certification Details	3
4	Requirements	5
4.1	Network Security Guidance.....	5
4.2	Network Security – Additional Steps	6
4.3	Host/Platform Guidance.....	6
4.4	Host/Platform – Additional Steps.....	7
4.5	Application Development Guidance	7
4.6	Operational Guidance.....	9
5	Getting Certified	10
6	What next?	12
7	Appendix A.....	13

1 Introduction

The philosophy of the AppExchange Certification Program is one that is inclusive, transparent and the foundation of trust for customers and partners.

AppExchange Certified applications not only integrate brilliantly with Salesforce.com but also adhere to stringent security requirements.

The AppExchange Certified logo demonstrates both Salesforce.com's faith in the application and the partnership in general.

We have had some great feedback from our customers who use the AppExchange Certified logo as a selection criterion, and from our partners who are doing exceedingly well with their certified offerings.

It is an indication of a true ecosystem where we help each other to succeed.

2 Why Certify?

By complying with the AppExchange Certification requirements partners not only meet their obligations to our security-conscious ecosystem, but also build a culture of trust that benefits everyone. From March 15, 2007 all new applications must be certified before getting listed on AppExchange and all the existing partner applications must get certified within the course of this year.

	Benefits of Certification
Everyone	Mitigate risk Greater confidence in certified applications
Partner	Positive image maintained Increased revenue and improved bottom line Happy customers
Customer	Information is safeguarded
Ecosystem	"Good security neighbors" encouraged

Additional Benefits for certified applications:

Prominence on AppExchange

AppExchange applications are more prominently featured as they are noted by the AppExchange Certified logo and appear first in category listings.

API Token for Professional Edition Access

Eligible¹ Certified solutions will receive an API token that allows partner API calls² to function with Professional Edition orgs in addition to Enterprise Edition and Unlimited Edition orgs.

¹ Integration brokers and EAI solutions are not eligible to receive PE-enabled API token

² API calls from SControls are not supported in Professional Edition.

3 AppExchange Certification Details

Application Types:

Currently, we certify the following 2 application categories:

Client/Software premise applications deliver application functionality by leveraging web services integration from desktop or server-based systems. These applications typically do not have any presentation in the salesforce.com UI. [Outlook Edition](#) and the [Ringlead DeClone](#) service are examples of Client applications.

On-demand Composite applications deliver application functionality by leveraging external Web services or applications in some way.

We have 2 certified hosting providers namely Opsource and Rackspace with whom we have worked out an AppExchange configuration package. For those on-demand composite applications using one of our **certified hosting providers** for managed hosting, the certification process will be slightly easier as we have already reviewed and approved them.

Native applications that are built entirely within the Apex platform do not need to get certified.

Test Categories:

The certification review tests are divided into the following 4 categories:

Network: We will review your network configuration, IDS, firewall, NAT etc.

Host: We will review your Operating System and other host configurations, patching, etc.

Application: We will review your application construction, authentication, software development lifecycle etc.

Operations: We will review whether you have a repeatable policies and procedures in place around change management, access control etc.

Test Types:

The certification process comprises of two types of assessments:

Qualitative Assessment:

This is a question and answer round where we will review your questionnaire response and conduct an interview. The questions will cover the above test categories. All applications will go through the interview round wherein, we will review the questionnaire response and see the functional demonstration of the integration touch-points between your application and Salesforce.com.

Quantitative Assessment:

Here we will conduct network and application penetration tests, wherever applicable, using standard tools.













For **software/client-premise applications** we will install the application and conduct application penetration tests. Some of the items we will review are:

- Whether credentials are transmitted in plain text
- Test credential encryption
- Check storage of customer data

For **on-demand composite applications**, we will conduct network and web-application penetration tests.

- Network Tests: We will use standard tools like NMAP and Qualys or Nessus. Some of the items the network tests will review are:
 - Open ports
 - Known vulnerabilities
 - Server configuration issues
 - Potentially validate IDS configurationWe may also conduct firewall and router configuration review.
- Web Application Tests: This is a combination of automated and manual testing. We will use standard tools like Paros, AppScan or Web Inspect. Some of the items the web-application tests will review are:
 - Injection flaws such as SQL injection or Cross-site scripting (XSS)
 - Recovery of credentials
 - Authorization controls
 - Potentially validate IDS configuration

Certification Matrix

	Software	On Demand (Certified Host)	On Demand
Network			 
Host			
App	 	 	 
Ops			



Questionnaire



System Tests

4 Requirements

As part of the Certification process, Salesforce.com critically reviews all new applications for compliance with Salesforce.com's Certification Requirements. Applications must meet or exceed these requirements to become certified. Existing certified applications will also be tested on an annual basis.

Below, we have outlined the rationale for taking care of security issues early and to provide you a framework for modeling your strategy in order to better prepare you for certification and to enhance your security and risk posture while preparing your solution for the marketplace.

4.1 Network Security Guidance

There is general network security guidance that is accepted by most information security professionals as a given whether it is designed to protect a collocation facility or to protect a corporate environment. At salesforce.com we do not deviate significantly from what is generally accepted as reasonable security. Below is what we consider an appropriate minimum and we will even discuss what you may want to consider as solutions that go beyond the minimum. You may be able to find solutions that integrate some of these requirements together that could meet your needs at a lower cost. Don't rule out multi-function devices unless the unit cannot maintain the desired level of performance:

Stateful Packet Inspection Firewall with NAT enabled

There are a large number of vendors who can satisfy this requirement.

Web/Application servers

Web/Application servers should be on a DMZ separated by a second firewall layer (logical or physical) from the database server.

Network IDS/IPS (Intrusion Detection System/Intrusion Protection System)

Many firewall vendors integrate IDS/IPS into their multi-function firewall.

Log Management

Automated log aggregation and alerting for all network devices and systems. Note: Manual review on a weekly basis is acceptable for certification; however, it is not scalable, error prone, and is very time consuming (costly). Database and Application logging should be enabled as well (for forensic purposes); however, salesforce.com does not require automated alerting or manual reviews of those logs. Log retention for at least 1 year to facilitate forensic investigations (7 Years if your organization or customers require longer).

Do not use wireless in collocation facilities.

Corporate implementations should include modern access control (e.g. WPA2 Enterprise) and wireless IDS.

4.2 Network Security – Additional Steps

If you are interested in providing an even more robust security solution, you may want to consider an Application Firewall (usually also includes an SSL offload) and/or Database Logging/IDS solution. These enhancements could further enhance security and potentially provide you with a comparative advantage over your competition. Additionally, by implementing these solutions, you could potentially compensate for a weakness in another area (e.g. A Database Logging solution could compensate for use of shared database user accounts by being able to track the underlying system account and logging that behavior to that unique system account).

4.3 Host/Platform Guidance

The guidance for system security should include no significant surprises. Salesforce.com is interested in making sure you are taking appropriate levels of care in securing systems and most will consider this obvious, common sense:

System configuration standard:

As noted below, salesforce.com expects partners to have a system configuration standard. This standard should include appropriate host hardening. Operating System manufacturers usually provide guidance around host hardening (such as the Windows Server 2003 Security Guide):

- Remove unnecessary services
- Harden services as required
- Remove/Rename default accounts and change passwords
- Encrypt all passwords
- Implement a robust password policy
 - Minimum 8 characters
 - Combination (3 out of 4) of numbers, letters (lower and upper) and special characters
 - Enable lock outs for bad attempts (3-5)
 - Enable password expiration (90 days)
 - Enable password history (don't allow reuse of last 8 passwords)

- Enable system logging and aggregate into log management system noted in Network Security Guidance (item 4). Alternatively, perform weekly log review. Log retention for at least 1 year to facilitate forensic investigations (7 Years if your organization or customers require longer).
- Enable host based firewalls to improve defense in depth.

Remote access

Remote access of systems in both remote and corporate environments must be secure. VPN tunnels or dedicated links should be used to remotely access any supported environment. SSHv2, IPSEC VPN, and SSL VPN are examples of mechanisms that would be appropriate. Persistent tunnels or dedicated links should have ACLs implemented to help ensure that only authorized users have access to secure remote computing infrastructure.

Patch Management Process

A documented and well followed patch management process is essential. Administrators should subscribe to one or more vulnerability e-mail lists and review recommendations at least weekly. Administrators also will review security recommendations from OS vendors and rollout recommended and critical patches after appropriate levels of testing and evaluation. For smaller implementations, a manual process for patch management is reasonable. As the size of the implementation grows, an automated solution could become important.

Anti-virus

All Windows servers will have an anti-virus solution implemented with automated updates of virus definitions. This should be a centrally administered solution, especially in larger implementations. Anti-virus should also be considered for non-Windows platforms, especially if files will be exchanged with Windows systems.

4.4 Host/Platform – Additional Steps

Consideration should be given to going beyond just the minimums noted above. A Host IDS solution could provide additional coverage and potentially compensate for other control weaknesses in your environment. Tools that lock configurations and/or alert on configuration changes could be useful for ensuring adherence to your Change Control policy. Encrypted file systems or databases could improve confidentiality. And an enterprise password vault could mitigate the risk of using shared passwords (especially shared passwords for privileged users).

4.5 Application Development Guidance

Developing a secure application is critical for services connected to Salesforce.com. To do this, there are a number of important items your organization should consider.

Software Development Lifecycle Management

Adherence to relevant policies is critical. Comply with your software development and change control policies. Also, ensure that your policies include appropriate code reviews, testing, and a strict methodology for rolling code to production, including appropriate segregation of duties that ensures that application development personnel do not have privileged access to the production environment.

Salesforce.com login credentials

As a general rule, do not store salesforce.com login credentials outside of the salesforce.com service. Instead, re-use the session ID in the resulting API calls. In addition, never pass credentials in the URL directly.

If the integration requires storage of salesforce.com admin login credentials, typically for performing batch calls and other asynchronous operations, the best practice is to request the customer to create a profile that can only login from the IP address of the server doing the synchronization. You must instruct your customers to provide a distinct API user and assign this user to that profile (additional cost may apply).

Password Encryption:

Passwords should be encrypted using a modern symmetric encryption algorithm such as AES, 3DES, Blowfish which uses a key strength greater than 128 bits or an asymmetric encryption algorithm such as RSA which uses a key strength of 1024 bits.

Use secure locations to store the key such as Java Keystore, which requires a password supplied by a user to be opened. Other suitable locations include Windows registry as long as there are ACLs (Access Control Lists) in place on the relevant registry key.

Encryption keys should be changed on a periodic basis and should not be reused across different environments such as testing, QA and production. The keys should be known or accessible by a restricted number of people and the keys should be stored in such a way as to prevent unauthorized access to the key material. If the keys are backed up, then all backup media should be stored in secure location.

If you persist customer data outside of the salesforce.com service (either through synchronization or by storing the user's salesforce.com password), disclose this information to the customer and state this clearly in the terms of use and privacy policy for your application.

Since salesforce.com passwords can be set to expire at variable intervals, you must handle invalid password exceptions in a manner that does not interfere with the standard use of salesforce.com. Obfuscate the password and do not store it outside of salesforce.com. Draw the users' attention to the fact that they should look for the salesforce.com URL and other distinguishing features to avoid getting phished.

Note that salesforce.com employs a lockout mechanism after a number of failed login attempts, so care should be taken not to retry failed login credentials.

Application username and password management

Likewise, ensure that your own application username and password management is secure. Use one-way hashing mechanism like MD5, SHA1, SHA256.

Authentication and authorization mechanism

Spend time planning and documenting how you will perform authentication and authorization. Good planning will result in a better, more secure, implementation. Make sure that you have a robust password management mechanism. For example, if the application password is changed, make sure that the authentication logic is still valid.

If deploying components to clients, run anti-virus prior to bundling up the package for distribution. It also isn't a bad idea to run anti-virus prior to rolling your application into your own environment.

Dynamic SQL

Avoid Dynamic SQL. If you choose to use Dynamic SQL anyway, please communicate that to the person performing the Salesforce.com security review and be prepared with a detailed rationale for doing so and your methodology for minimizing the risk to customer data.

Input validation

Perform validation on all input fields. Successful attacks on applications frequently are the result of unforeseen input being accepted by the system and then leaving it up to the application or database server to figure out how to deal with it. Perform security by design and ensure that your application is protected from common application vulnerabilities such as SQL injection, cross-site scripting, buffer overflow etc.

Application Development – Additional Steps

You should also investigate automated source code checking tools, SQL tools, and possibly even application firewalls and database IDS/Logging solutions (also mentioned in the Network Security section). These tools may help mitigate weaknesses in your overall controls for application development and provide additional assurance that customer data is secure. See Appendix A for the entire tools list.

4.6 Operational Guidance

Each environment is different; however, some operational considerations are universal. We are interested in making sure you follow important operational rules without impacting how the specifics of your solution functions in your environment.

Procedure Documentation and Change Management

It is extremely important to align your policies with your operational behavior in such a way as to maximize the risk mitigation intended by that policy while not significantly impacting your ability to provide your service. This alignment between policy and behavior will allow auditors the ability to validate that you are following your policies.

Incident Response

You must actively monitor your network. In the sections above, you will note that we talk about review of logs and alerting. That is part of this. Additionally, you need to implement solutions to actively monitor your network and systems so that availability issues are addressed early and quickly in accordance with your Incident Management process.

Business Continuity and Disaster Recovery

Business Continuity and Disaster Recovery are frequently considered the same thing, they are not; however they are interrelated. Your organization not only needs plans for both, it is also important to exercise the plans in order to determine whether they will work when they need to. Testing should occur annually; however, it is not unreasonable to conduct a less strenuous walkthrough exercise instead of a full test in the year following a successful full test.

Disaster Recovery – This plan should cover the data, hardware, and software necessary to restart operations after a natural or human-caused disaster. Additionally, it should cover the unexpected loss of key personnel necessary to carry out the plan.

Business Continuity – This is typically a more comprehensive plan that includes how the organization as a whole will resume partially or completely interrupted critical functions within a predetermined time after a disaster or disruption. The plan usually includes all aspects of the business including Customer Support, Finance, IT, Sales, etc.

Employee Training

Proper employee training can head off many operational crises. Training is important for all employees as well as those responsible for the security architecture.

It is important that you set aside an hour each year (minimum) to delve into security concerns at your organization. These security classes for your employees should cover the policies and your company and behaviors you expect as well as critical vectors for security incidents so that they can help secure your organization's critical data and infrastructure.

Employees responsible for implementing the information security program at your organization should also refresh their training annually by participating in conferences, seminars, and classes focused on security. These employees should dedicate at least one to two weeks each year learning and refreshing their skills.

Password Policy

We note in the password policy section that passwords should be rotated every 90 days. When it comes to encryption keys, these should also be rotated according to a schedule (not less than annually – more frequently if a risk analysis indicates it would mitigate additional risk to do so). Additionally, encryption keys and certificates should be stored in an appropriate secure location outside of your production environment.

Logging in via the API

If you use a Custom Link (or S-Control) to invoke an external operation and the external system requires API access to the Salesforce.com platform, ensure that you pass the `serverUrl` and current session ID as query parameters (implemented as a merge field) to obviate the need for the login call.

If you exercise the `login()` call, be sure to call the single logon server (<https://www.salesforce.com>) and not any of the service instances directly.

There should be only one login per session and `salesforce.com` will return a session ID to you upon successful login. The session length is based on the org setting (between 30 minutes and 8 hours). The session expires a set time after it is created and it is not an idle timeout.

SSL (HTTPS)

Always use HTTPS as the transport for communication with the Web service. If the solution renders data in the `salesforce.com` UI (Custom Link or S-Control), SSL-enable the site using a valid certificate so as to avoid the browser warning of crossing mixed security zones.

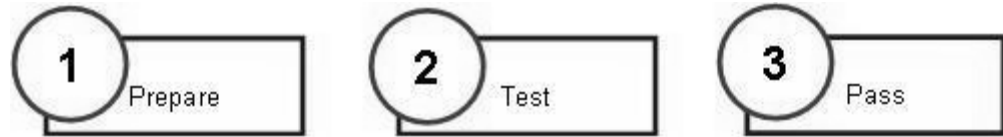
(Internet circuits, routers, switches, firewalls, load balancers, SSL accelerators, host systems, storage), and/or a disaster recovery plan should be in place.

Conclusion

Security of customer information is absolutely critical for our mutual continued success. It is necessary to do the right thing from the very beginning to help our customers remain confident that AppExchange is a desirable, trusted platform for their core corporate applications.

5 Getting Certified

Certification Process



Phase I – Prepare

Step 1 – Request to certify:

To certify the application you need to be a partner first.

Complete the [“Become a Partner” contact form](#) and indicate interest in certifying your AppExchange application.

Your PSR (Partner Success Representative) will send you the pre-qualification survey to determine the state of readiness of your application and help identify your application type (Software/Client Premise, On-demand (certified hosting provider) or On-demand (other)).

Based on your response, your PSR will send you an email with the Certification Welcome Kit providing instructions and guidelines on the certification process. The kit also contains the certification agreement and certification questionnaire.

Step 2 – Prepare for AppExchange Certification:

Visit the [AppExchange Certification Wiki](#) for the latest certification information such as the recent webinar, FAQs etc.

Visit the [AppExchange Developer Network](#) for sample code and API documentation to assist in learning and implementing the AppExchange technologies.

Review and implement the requirements mentioned in section 3 in the Welcome Kit.

Execute dry run network and application penetration tests using standard tools where applicable. Review and fix all high and medium risk vulnerabilities detected during the tests.

Step 3 – Review and submit certification agreement and Purchase Order:

Review the certification agreement to ensure that you have understood and agree with the terms and conditions. You may request for a meeting to discuss the agreement and to set general expectations around the program and benefits.

Submit the executed certification agreement and P.O. via fax to: (415) 335 4080. The General Counsel will review, counter-sign and mail it back to you.

Your PSM (Partner Success Manager) will then schedule the certification review meeting.

Phase II – Test

Step 4 – Submit your certification questionnaires:

Complete the certification questionnaire and email it to the CM (Certification Manager) a week prior to the meeting date.

Step 5 – Qualitative Assessment:

Organize all the appropriate technical resources to attend the meeting. We recommend all those who completed the questionnaire response to attend. For on-demand applications, it may also be a good idea, to arrange for a contact from the hosting provider to attend. This would expedite the process should there be specific questions around the network and host infrastructure.

Based on the review, we may have follow-up questionnaires so that we have enough information to make our decision.

We request all partners to be proactive during the review period and provide any additional documentation or follow-up questions so that we can complete the process within the 2-3 week timeline.

Step 6 – Quantitative Assessment:

Based on the outcome (see Results below for details) of the Qualitative Assessment, we will then conduct the appropriate Quantitative Assessment.

Phase III – Pass

Step 7 – Certification Status:

The Primary contacts on your account will receive an email once your certification review is complete.

If you pass or provisionally pass the Qualitative Assessment stage, then we will immediately follow it with the Quantitative Assessment stage.

If you fail the Qualitative Assessment stage, then we will work out a mutually agreed upon timeframe for you to remediate the vulnerabilities found. We will also assist you with the necessary security consultation should you require so. Upon the timeline passing, we will review the remediation and follow with the Quantitative Assessment stage.

Similarly, if you fail the Quantitative Assessment, we will work out a suitable timeline to remedy as well as provide security consultation should you need further assistance. We will review the remediation at the end of the timeline.

On passing certification, we will send an email containing the certification logos and API token that enables you to access a wider set of customers.

We will also place the certification logo on your AppExchange listing.

6 What next?

Certification Review Timeline:

The Certification process should not take more than 10-15 business days provided:

- Your documentation is complete and accurate
- You have met the certification requirements
- You are within the agreement guidelines

Re-Certification Review process:

Re-certification is conducted on a yearly basis. Submit the executed agreement, P.O. and certification questionnaire. Review process is similar to first-time certification process.

In the event that there is no change in the application, CM may conduct random tests (see Random Testing below).

Review process for multiple applications on same infrastructure:

Partners with more than one application to certify can certify multiple applications built on the same infrastructure.

The process will be shorter as the operations and network infrastructure reviews would have been conducted during the certification of the first application. We will mainly review the application layer. We may conduct a Quantitative Assessment.

Random Testing:

Although certification is an annual process, salesforce.com reserves the right to conduct random tests on certified applications on the AppExchange.

If during these tests, CM finds that the application has deviated from any of our best practices requirements, we will notify and provide the partner some time to remedy the issue. In extreme cases, we may revoke the certification designation and pull the AppExchange listing from public viewing.

7 Appendix A

Below is a list of security tools. We highly encourage you to test your applications using these tools prior to your certification review:

Network Penetration Test tools:

- Nessus
- Nmap
- Amap
- Therut

Web Application Penetration Test tools:

- AppScan
- Paros
- Web Proxy

Application security tools:

- Fortify Software (SCA, Tracer, Defender)
- Ouncelabs