



Frequently Asked Questions

ManageSecure – Frequently Asked Questions

What is ManageSecure?

ManageSecure is a software product that enables you to secure your Intranet and Internet based applications, and to manage your security resources.

How does ManageSecure secure my network?

ManageSecure applies authentication, access control and public key cryptography technology to identify, authenticate and authorize end users and control their access to various web resources. It also provides tools to secure and manage commonly used security resources.

What type of Organizations may use ManageSecure?

Corporations that deal with sensitive or mission critical information and want to ensure that only a designated user (or group) can access a particular web application or resources.

My organization uses a firewall that blocks accesses from the web. Why do I need ManageSecure?

Most security attacks come from within the Intranet. Firewalls are not adequate for protecting the Intranet assets from these attacks. Some security attacks are made over port 80 (http) or 443 (https). Typically firewalls permit traffic on these ports. Further, Firewalls are not adequate to control access based on URLs. ManageSecure provides this additional access control over your web resources.

Does ManageSecure replace a traditional firewall?

No. It only complements a firewall by adding an additional security layer.

Does ManageSecure protect both Intranet and Internet applications?

Yes. ManageSecure has access control components that can protect both Intranet and Internet applications by controlling access at the web-server layer.

My organization has application X that has a login mechanism. Why do I need ManageSecure?

Having each application implement its own authentication mechanism creates disparate, hard to manage, and often inconsistent enforcement of security policies. Having a common, standards based security solution allows you to have a consistent, centrally managed security policy across your Intranet. ManageSecure provides such a solution.

What kinds of security threats are addressed by ManageSecure?

- Unauthorized access to URL based applications both from within the organization and from outside
- Internet sniffing attacks (e.g., passwords, credit card information, or other sensitive data)



Frequently Asked Questions

- Password compromise due to large number of poorly managed passwords
- Denial of service due to lost passwords

What types of access control does ManageSecure offer for web applications?

At the most basic level, ManageSecure can use plain login/password to identify and authenticate the user, and control access to web resources based on this identity. Beyond this, ManageSecure can also enable SSL based communication. Further, ManageSecure can offer strong security by managing client-side certificates (i.e., full PKI support), and using the strong authentication based on client certificates to control access to web resources. ManageSecure can define access roles and privileges, hence it supports Role Based Access Control (RBAC).

What additional features are in ManageSecure?

- Password management
- Keystore management
- Encryption management
- LDAP management
- Certificate management
- Certificate request management
- Trust relation management
- Monitoring of web and application servers for various error conditions

What security standards does ManageSecure conform to?

- Security Assertion Markup Language (SAML)
- X.509 Certificates and CRLs
- PKCS12 Keystores
- PKCS7, Base64 or DER Certificates
- PKCS10 Certificate Request
- JKS Trust Stores
- PEM private keys
- SSL
- LDAP
- Kerberos/Active Directory
- Java Authentication and Authorization framework

What web-servers can ManageSecure access control filter be used with?

- Microsoft IIS
- Apache (Solaris 5.9 Sparc, Redhat Linux 8.0)

What type of security expertise is needed to run ManageSecure?



Frequently Asked Questions

A good UNIX or Windows network administrator can be trained to install and operate ManageSecure. For organizations using strong security, administrator should have a high level knowledge of PKI and X.509 certificates.

What does ManageSecure cost?

Please contact kailar@bnetal.com or abnipl@vsnl.com for pricing information.

How can I obtain more information on ManageSecure?

Please send in your enquiries by email to kailar@bnetal.com, or abnipl@vsnl.com.

What is single sign-on?

When using multiple instances of web-servers on a network (e.g., each may be hosting a different application), the ability to authenticate a user at one point in the network and to propagate the user session to all subsequent web-servers throughout the network (without requiring additional logins) is called single sign-on. ManageSecure provides single sign-on capability.

How configurable is ManageSecure?

ManageSecure authentication policies are extensible using Java Authentication and Authorization framework, whereby you can define your own custom authentication mechanisms and plug them in. Also, Kerberos/Active Directory authentication and LDAP based authentication are supported. User interface layout is also configurable. You can edit the provided set of HTML pages to create custom look and feel for user interfaces.



Frequently Asked Questions

In what scenarios can ManageSecure be used?

ManageSecure can be used in several configurations based on the security and functional requirements of the organization where it is deployed. The following are some common usage scenarios:

Scenario 1:

Company A has no security critical applications on the web, but system administrators use several passwords, and need to generate self-signed certificates for some internal webservers. Company A uses ManageSecure Management Client to manage passwords, file encryption, to generate self-signed certificates, or to generate certificate requests to be sent to a third-party CA.

Scenario 2:

Company B needs to enable SSL on its web-servers, but does not need URL level access control. Hence it uses ManageSecure Admin Client to process certificate requests for its web-servers, and installs the certificates to make its web-servers SSL enabled.

Scenario 3:

Company C has several servers that need to be monitored on a 24/7 basis. Administrators who are on call should receive email on their handheld devices, and hence Company C uses ManageSecure Management Client to monitor its servers for error conditions, certificate expiration etc, and send email alerts to administrators when there is a problem.

Scenario 4:

Company D has a small number of users and small number of security critical applications. It requires strong authentication, but since the number of users is small they can be mapped to local users on the web-server. It uses ManageSecure Admin Client to manage a full PKI, including client certificates, CRLs etc. It uses its web-servers' native authentication in conjunction with the PKI (i.e., it does not use Access Control Filter).

Scenario 5:

Company E has several web applications and access to these must be tightly controlled. However, communication confidentiality (i.e., SSL based encryption) is not a high priority for this company, as the applications are accessed only within an Intranet, and most users are trusted. Hence Company E uses ManageSecure Access Control Filter to manage access to its web resources. It does not use ManageSecure PKI features for access control (i.e., it uses login/password authentication only).



Frequently Asked Questions

Scenario 6:

Company F has some sensitive applications being accessed via their web portal on the Internet. Hence, communication confidentiality (i.e., SSL) is very important. However, Company F is satisfied with login/password based authentication. Hence Company F uses ManageSecure Access Control Filter to manage access to its web resources. It uses ManageSecure to SSL enable its web-servers, but does not use a full PKI (i.e., it does not use client certificates. It uses login/password authentication only).

Scenario 7:

Company G has strong authentication and confidentiality requirements for its web applications. However, it already has a third party that acts as its Certificate Authority for issuing certificates, and wishes to continue using that CA. Hence Company G uses ManageSecure Access Control Filter along with the third-party PKI to implement strong access control based on client certificates.

Scenario 8:

Company H has strong confidentiality, authentication and authorization requirements. It has no third party arrangements with any CA, and wishes to act as its own CA (this way it will have better control over the certificate management process). It uses ManageSecure Access Control Filter along with ManageSecure PKI to implement strong access control based on client certificates.

Scenario 9:

Company I has strong confidentiality, authentication and authorization requirements. It has limited network administration staff and hence wants the certificate authority functions to be out-sourced. It uses ManageSecure Access Control Filter, but uses a third party firm that has a ManageSecure CA to generate and manage client certificates.



Frequently Asked Questions

Public Key Infrastructure FAQ

What is a Public Key Infrastructure (PKI)?

A public key infrastructure consists of a certificate authority, and a group of users that trust the certificate authority to issue certificates for the purpose of identifying or authorizing users in the network. Typically a PKI also contains tools to locate, manage, and revoke certificates.

What is a Certificate?

A certificate is a binary file that contains some information about the user (such as the user's distinguished name), and a signature by a trusted party (e.g., certificate authority). Certificates in ManageSecure conform to X.509 standard. X.509 certificates can be processed by any standard browser or web-server.

What is a Certificate Request?

A certificate request is a binary (or ASCII encoded) file that contains information needed by the certificate authority to generate a certificate. Certificate requests can be generated from the ManageSecure browser based form, or from the ManageSecure admin client, or from within the IIS webserver (in this last case, the certificate request is only used for generating a web-server certificate).

What is a Certificate Revocation List (CRL)?

A certificate revocation list is a file that contains a list of certificate sequence numbers of those certificates that have been revoked, along with a signature by a trusted party (e.g., Certificate Authority). CRLs in ManageSecure conform to the X.509 standard.

What is LDAP?

LDAP stands for Lightweight Directory Access Protocol. It is a standard way to organize information in a hierarchical model and to query information.