nCrypted Cloud

Success Criteria for Evaluating nCrypted Cloud

Prepared By: Nick Stamos / Revision Number: 1.0

Contents

Version History

Name	Revision	Date	Details
Nick Stamos	1.0	08/28/2013	
Tom Murphy	1.1		

Purpose

The assessment involves checking whether nCrypted Cloud, and the data security initiative it supports, conforms to various requirements and exhibits qualities that are expected of an enterprise security solution. The more characteristics that are satisfied, the more suitable nCrypted Cloud would be to improve the organization's security posture.

In performing the evaluation, customers are encouraged to consider how different user classes affect the importance of the criteria. For example, for Usability, a small set of well-defined, accurate, task-oriented user documentation may be comprehensive for business users but inadequate for technical users or software developers. Assessments specific to user classes may further define requirements of specific user classes to be factored in and so, for example, show that a use case rates highly for business users but poorly for developers, or vice versa.

Evaluation Criteria

Architecture & Platform Support

Webpage: https://www.ncryptedcloud.com/ under 'Seamless Cloud Integration'

Cloud based solution is always available and accessible from corporate network and remote locations using secure protocols (HTTPS)	☐Success ☐Failed
nCryptedCloud client implementation supports inherent designs of operating system and does not attempt to override them	☐Success ☐Failed
nCryptedCloud Client supports organization's preferred operating systems (Windows and Mac)	☐Success ☐Failed
nCryptedCloud Client supports popular operating systems for handhelds (Android and iOS)	☐Success ☐Failed
nCryptedCloud administrative console can be managed using popular browsers like Internet Explorer, Safari, Chrome and Firefox	☐Success ☐Failed

Corporate Deployment

User Manual page: 30/Mac, 22/Windows

nCryptedCloud client installer can be customized to display corporate logo and custom messages to users	☐Success ☐Failed
nCryptedCloud client installer can be distributed to managed endpoints through software distribution solution (e.g. BigFix, LanDesk, CA Unicenter, etc.)	☐Success ☐Failed
End users can be automatically provisioned to use the corporate nCryptedCloud client on their workstations without user interaction	☐Success ☐Failed

nCryptedCloud Client supports popular operating systems for handhelds (Android and iOS)	☐Success ☐Failed
Standard nCryptedCloud client can be installed by end user with minimal instructions	☐Success ☐Failed
Corporate nCryptedCloud client can be installed by users with minimal input	
Deployment progress of corporate nCryptedCloud clients can be monitored in nCryptedCloud admin console	☐Success ☐Failed

Securing Files

User Manual page: 14/Mac, 9/Windows

Encrypt files own use: User can secure their files by encrypting designated folders. Right-click on selected Dropbox folder, go to nCryptedCloud > Make Private. Folder should be encrypted for personal use only	☐Success ☐Failed
Apply sensitivity to files: User can apply sensitivity to files. Right-click on selected Dropbox folder, go to nCryptedCloud > Sensitivity and select one of the four (Low, Medium, High, Top Secret) levels and confirm when prompted. Folder is encrypted and files within the folder have the sensitivity level applied	☐Success ☐Failed

Secure Collaboration

User Manual page: 23/Mac, 16/Windows

Share securely: Dropbox folders currently shared with others can be encrypted allowing sharing the files securely. Right-click shared folder in Dropbox and select 'Share Securely'. Files in the folder are encrypted. Users sharing the folder will now be required to use nCryptedCloud (Personal/Enterprise edition) to view the files	☐Success ☐Failed
Manage Sharing: User can remove shared access to other users and make files in shared folder private. Right-click on securely shared folder and select 'Remove shared access'. Files in the folder are no longer viewable by other users	☐Success ☐Failed
Manage Sharing Selectively: User can view and manage shared access to a folder for specific users. Right click a shared folder and select 'Shared with…' option. In the 'Folder Sharing Information' window, select the user to whom access needs to be revoked, select 'Closed' under Folder Membership and then click 'Apply'	☐Success ☐Failed

Trusted Sharing

User Manual page: 16/Mac, 10/Windows

Share Files Securely with non-Dropbox Users: "Trusted Sharing" allows nCryptedCloud users the ability to share encrypted files with anyone on a one-off basis via the nCryptedCloud portal, mobile device or workstation. Right-click a file and select 'Trusted Sharing…'. In the Trusted Sharing window, type in email address for the recipient with whom the file needs to be shared.	☐Success ☐Failed

Select to set permissions for download and watermark the file (applicable to PDF and image format files only) and set expiration time and custom message for the recipient if desired. Recipient receives an email with the link to view the file, note expiration and watermark settings you selected are applied when the file is viewed and as the file owner, you receive an email with audit trail indicating the recipient viewed/downloaded the file you shared securely.	

Device Management

Refer page XX of user guide

Unlink Devices: Ability to unlink lost devices or devices of employees no longer associated with the organization is critical for securing the data on the devices. Log into nCryptedCloud portal, go to Settings > Devices. Select the device you desire to unlink. Encrypted data on this device will no longer be readable to the user.	☐Success ☐Failed

Policy Management

User Manual page: 14/Mac, 9/Windows

Apply/Remove Privacy to Folders: Having control of encryption for the files is critical to managing security and collaboration. nCryptedCloud allows users to apply and remove privacy on their own folders as and when needed. From nCryptedCloud view, right-click a folder and select to 'Share Securely..' or select to 'Make Private' to encrypt the files. If the folder is already private or shared securely (i.e. encrypted), select to remove privacy, the files are immediately decrypted and returned to unencrypted state.	☐Success ☐Failed

Multi-Identities

User Manual page: 31/Mac, 22/Windows

Add Multi-Identity: nCryptedCloud gives users the unique ability to associate multiple identities so personal and corporate files are treated with respective privacy policies. Users can apply privacy settings to their personal files while corporate files acquire policies defined by the administrator. Log in to nCryptedCloud web portal, go to Identities under your account and select to add new identity. Enter the email address associated with the organization (email address should match with the organization's domain). Confirmation email is sent to the email address provided. After confirming the email address, the user now has the option to associate folders to personal or corporate identity.	☐Success ☐Failed
Apply Identity to Folders: After adding corporate identity to your profile, right-click a folder, go to nCryptedCloud > Identities and select either the personal identity or corporate identity to make respective user the owner of the file. Confirm when prompted, and you will notice files in folder are automatically encrypted and the correct identity is now assigned as the owner of the folder.	☐Success ☐Failed

Change Identity of Folders: To change ownership of a folder, right-click the folder, go to nCryptedCloud > Identities and select the new identity to which you desire to associate the folder. Doing this will result in making that user the owner of the folder, who will then have the ability to apply privacy controls	☐Success ☐Failed

Enterprise Forensic Auditing

User Manual page: 30/Mac, 21/Windows

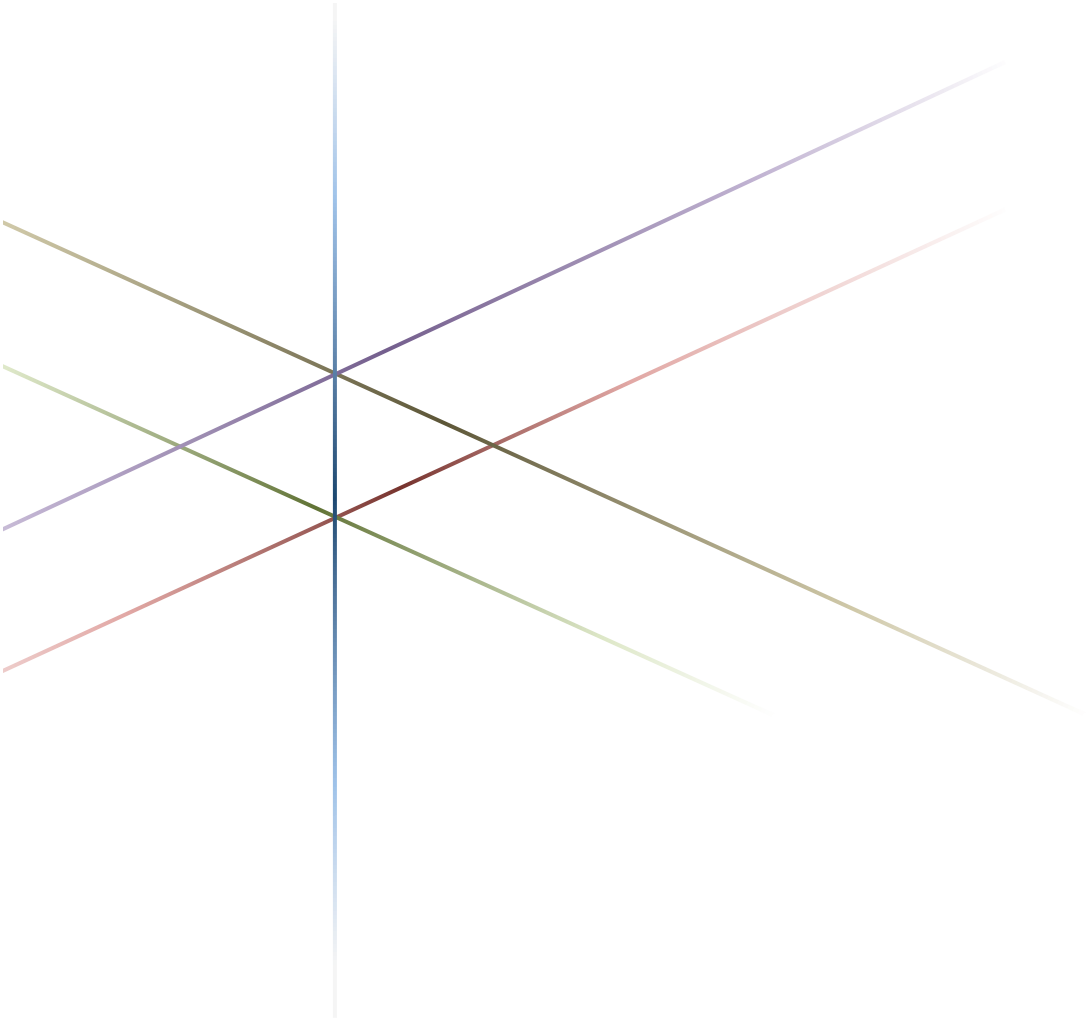
Manage Admins: To enable administrative rights for a user to organization's nCryptedCloud profile, log into nCryptedCloud portal, select 'Organizations' link under your user name. For organization displayed on the page, select 'Choose Action' > 'Manage admins'. In the Manage admins window, click on 'Make admin' button for the user whom you desire to assign administrative rights and then click 'Apply'. The user can now login to nCryptedCloud to manage the organization's users, devices and view reports	☐Success ☐Failed
Auditing Files Usage: Login to nCryptedCloud portal as administrator, click on 'Manage Team' button. In the organization's main page, click on 'Auditing' button on top row of the table. Current user activity events are displayed in the report.	☐Success ☐Failed
Search File Access: Login nCryptedCloud, go to Auditing screen and select 'Search' link. Type in a file or folder name to search. File activity associated with the file/folder is displayed in the results	☐Success ☐Failed
Organization Dashboard: Login nCryptedCloud, go to Auditing and select 'Statistics'. This page displays the trend of file activity for the organization, list of devices with nCryptedCloud that have been most active, Files that have been used the most, users that have been most active and the actions that users are performing the most.	☐Success ☐Failed

Compliance Support

User Manual page: 27/Mac, 19/Windows

User Access Revocation: A user's access to shared folder can be removed to support compliance needs where it is required to demonstrate unauthorized users should no longer have access to files they do not need access to. Right click a shared folder and select 'Shared with…' option. In the 'Folder Sharing Information' window, select the user to whom access needs to be revoked, select 'Closed' under Folder Membership and then click 'Apply'	☐Success ☐Failed
Device Revocation: A lost device or a device no longer associated with the organization may continue to store the organization's data. To revoke access to files on such devices, unlinking of the device to the organization can be performed. Log into nCryptedCloud portal, go to Settings > Devices. Select the device you desire to unlink. Encrypted data on this device will no longer be readable to the user.	☐Success ☐Failed
Revoke User Association with Enterprise: When a user is no longer associated with the organization, his/her relationship can be terminated in nCryptedCloud thus resulting in the user being denied access to any files/folders designated as being owned by the organization/organizational	☐Success ☐Failed

identity. To unassociated an user form the organization, log into nCryptedCloud portal, click on Manage Team and select to 'Remove' for under 'Choose Action' drop down for the specific user.	
Auditing Files Usage: Login to nCryptedCloud portal as administrator, click on 'Manage Team' button. In the organization's main page, click on 'Auditing' button on top row of the table. Current user activity events are displayed in the report. The report could be exported/printed to demonstrate compliance	☐Success ☐Failed



Enterprise Security Meets Consumer Simplicity.

nCryptedCloud seamlessly integrates with Cloud Storage Services to protect your data and privacy. nCryptedCloud acts as a layer on top of your current cloud storage service, giving you the ability to use nCryptedCloud without having to move any of your existing cloud data.

nCryptedCloud, 470 Atlantic Ave, Boston, MA 02210 Phone: (617) 520-4120

www.ncryptedcloud.com