

Domino Web Access und Sicherheit

Domino Web Access bietet eine ideale Möglichkeit, Notes Anwendungen über das Internet nutzen zu können. Damit entfällt die Notwendigkeit, die Notes Client Software installieren zu müssen. Das hat dann auch unweigerlich zur Folge, dass Sicherheitsmechanismen, die auf dem Notes Client basieren, nicht vorhanden sind. Doch wer will heutzutage schon auf Sicherheitswerkzeuge verzichten – gerade wenn es um unternehmensinterne Daten geht?

Natürlich bietet Domino Web Access eine Alternative zu den Domino und Notes spezifischen Sicherheitsmechanismen, welche die Verbindungen zwischen Domino Servern und Notes Clients sicher machen. Beispiele dazu sind Zertifikate und Verschlüsselungen. Allerdings sollte man sich in jedem Fall im Klaren darüber sein, dass alle Sicherheitseinstellungen, die im Domino Web Access vorhanden sind, nicht in der Lage sind, eine mit einem vollwertigen Notes Client verfügbare Sicherheit bieten zu können.

Bei dem Einsatz von Domino Web Access benötigt jeder Benutzer, der mit dem Domino Server arbeiten will, einen entsprechenden Benutzereintrag in dem Domino Directory oder einem anderen Verzeichnis, das für die Domino Authentifizierung verwendet wird. Außerdem ist für den Zugriff auf Domino Daten mittels Domino Web Access eine Notes ID erforderlich, damit auch die Offline Datenbank mit dem Server repliziert werden kann. Außerdem muss sich jeder Benutzer natürlich auch für den Zugriff auf die Domino Daten ausweisen in Form einer Kennwortgebundenen Anmeldung. Diese Anmeldung benötigt ein Internetkennwort, das im Personendokument des jeweiligen Notes Benutzers anzulegen ist. Mit diesem Internetkennwort erfolgt die Authentifizierung für Domino Web Access.

Notes
Person: WWinzig/Zebis/de

Basics | Work/Home | Other | Miscellaneous | Certificates | Roaming | Address Book

Basics

First name:

Middle name:

Last name:

User name:

Alternate name:

Short name/UserID:

Personal title:

Generational qualifier:

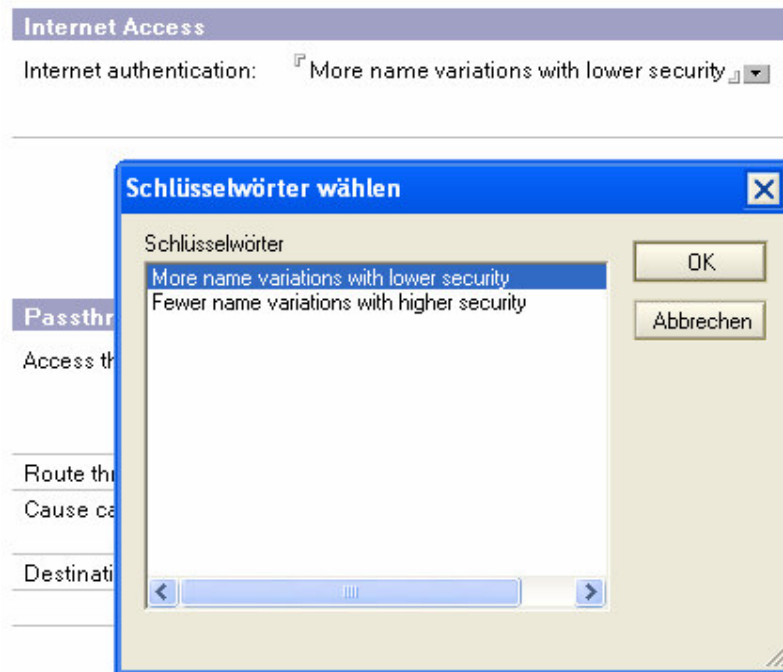
Internet password:
(A77772D0B2A4ECA17C4CEDD859E10F7F)

Preferred language:

001 Das Internetkennwort in dem Personendokument

Domino bietet die Möglichkeit, die Anmeldeinformationen, die bei einer Domino Web Access Verwendung benötigt werden, in einem gewissen Rahmen anpassen zu können. So lassen sich zum Beispiel auch die Kennwortsicherheitsstufen speziell für die Verwendung von Internetkennwörtern in dem Konfigurationsdokument des Servers definieren.

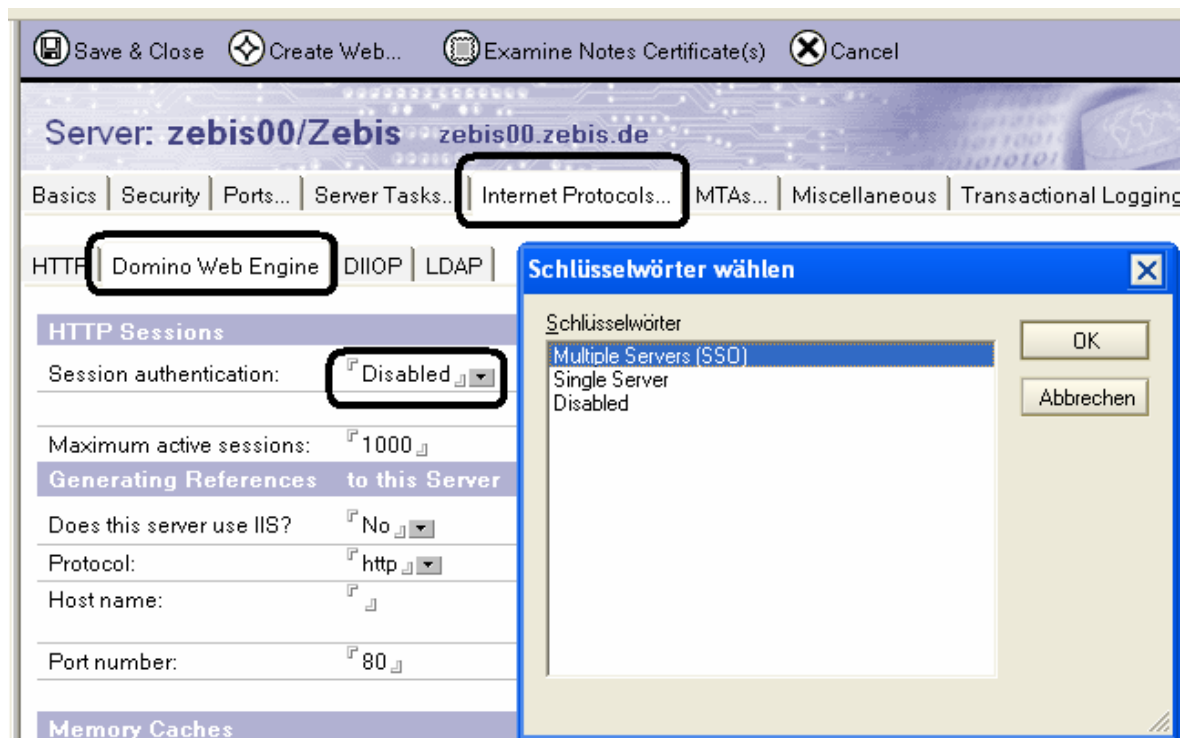
Die erforderlichen Einstellungen können sie in dem Serverdokument in dem Abschnitt „Security / Internet Access“ festlegen. In dem Feld „Internet authentictaion“ können sie festlegen, ob bei der Internetanmeldung einfache Namen verwendet werden dürfen, oder ob die Anmeldung nur mit einem qualifizierten und komplexeren Namen möglich ist.



002 Namenssicherheit

Leider ist die Anmeldung in diesem Bereich auf den Server und die Browsersitzung begrenzt. Das ist auch der Grund, weshalb bei einem Zugriff auf eine Datenbank, die auf einem anderen Server liegt, eine erneute Anmeldung erforderlich ist. In diesem Zusammenhang kann eventuell eine Single Signon (SSO) Lösung helfen.

Die Einstellungen, die solche „kleinen“ SSO-Ansätze ermöglichen, finden sie in den Konfigurationseinstellungen für den Domino Web Server. Per Standard ist für jeden Server für die http Authentifizierung „Disabled“ eingestellt. Um diese Einstellung zu verändern, wählen sie das Server Dokument und darin in dem Bereich „Internet Protocols / Domino Web Engine“ in dem Feld „Session authentication“ den Wert „Multiple Servers (SSO)“. Wenn sie diese Einstellung wählen, dann genügt eine Anmeldung an Domino Web Access unabhängig davon, ob sie auf Daten in dem Verzeichnis zugreifen, das auf dem Server liegt, an dem sie sich authentifiziert haben, oder ob sich diese in einem anderen Verzeichnis auf einem anderen Server befinden. Damit ist natürlich keine vollständige Domino SSO realisiert, sondern lediglich die Domino Web Access Besonderheit in Bezug auf die Anmeldung ein wenig umgangen worden.



003 http Authentifizierung ändern

Der Browser, der für den Domino Web Access Zugang verwendet werden soll, müssen einige kleiner Sicherheitseinstellungen beachtet werden. Unter anderem müssen für den Browser die Cookies aktiviert werden, wenn die SSO Einstellungen verwendet werden sollen.

Natürlich gelten bei der Verwendung von Domino Web Access die allgemeinen Empfehlungen, die Allgemeingültigkeit bei dem Zugriff auf sicherheitsrelevante Daten haben: Verzichten sie auf das temporäre Speichern von Informationen, die über das Internet abgerufen werden. Der Browser kann nämlich an dieser Stelle nicht differenzieren, ob es sich um sensible Daten oder unwichtige Daten handelt.

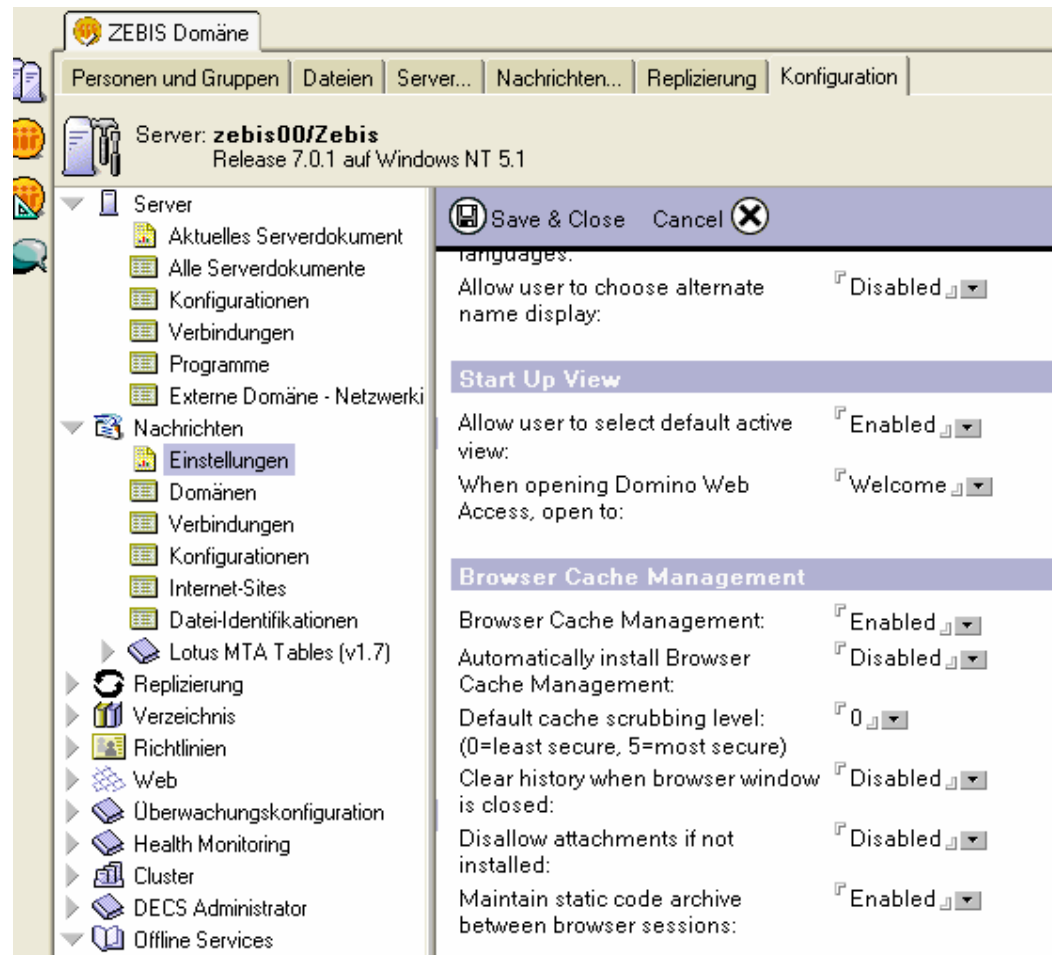
Ein weiterer Sicherheitskritischer Punkt bei dem Einsatz von Browsern ist die Möglichkeit, die Cache Funktionen des Browsers nutzen zu können. Diese sind zwar in vielen Bereich hilfreich und auch zum Teil unbedingt erforderlich, stellen auf der anderen Seite aber auch ein gewisses Sicherheitsrisiko dar – denn Informationen, die auf diese Weise „still und heimlich“ gespeichert werden, könnten durchaus von Unberechtigten ausgelesen und verwendet werden. IBM bietet für die Bereinigung des Caches nach dem Beenden von Domino Web Access mehrere Möglichkeiten.

Zum einen können sie über die Einstellungen für den Domino Web Access Server festlegen, dass bei dem Verlassen des Browsers bzw. der Anwendung eine besondere Webseite ausgegeben wird, mit deren Hilfe sich der Inhalt des Browser Caches gelöscht werden. Die Ausgabe einer solchen „Ende – Webseite“ können sie mit Hilfe der notes.ini Variablen „iNotes_WA_LohoutRedirect“

Außerdem sollten sie für den Einsatz von Domino Web Access das Browser Cache Management aktivieren. Damit wird verhindert, dass nach dem Beenden von Domino Web Access Sicherheitsrelevante Informationen im Cache erhalten bleiben und damit unter Umständen durch Unberechtigte verwendet werden kann. Zwar könnten Anwender auch die Bereinigungsoptionen verwenden, welche für eine Cache Leerung für jeden Browser angeboten werden, allerdings ist das unter Sicherheitsbetrachtungen kein wirklich gangbarer Weg. Neben den Browser eigenen Einstellungen, welche die Behandlung von temporäre gespeicherten Informationen und die Cache Behandlung angeht, bietet IBM seit der 7er Version auch eine von Domino gesteuerte Cache Verwaltung an, die bei einer Beendigung der Sitzung

den Cache Inhalt der Sitzung leert. Dabei werden die entsprechenden Einstellungen von dem Domino Server in den Browser übertragen und dort aktiviert.

Diese Cache Verwaltungsoption lässt sich in dem Konfigurationsdokument des Domino Web Access Servers (Nicht in dem Domino Server Dokument selbst!) einstellen. Sie finden dieses in dem Domino Administrator im linken Navigationsbereich unterhalb des Abschnittes „Messages“ (bzw. Nachrichten). Wählen sie diesen Abschnitt aus. Dort finden sie in dem Abschnitt „Domino Web Access“ unter anderem auch den Bereich „Browser Cache Management“, in dem sie die erforderlichen Einstellungen vornehmen können



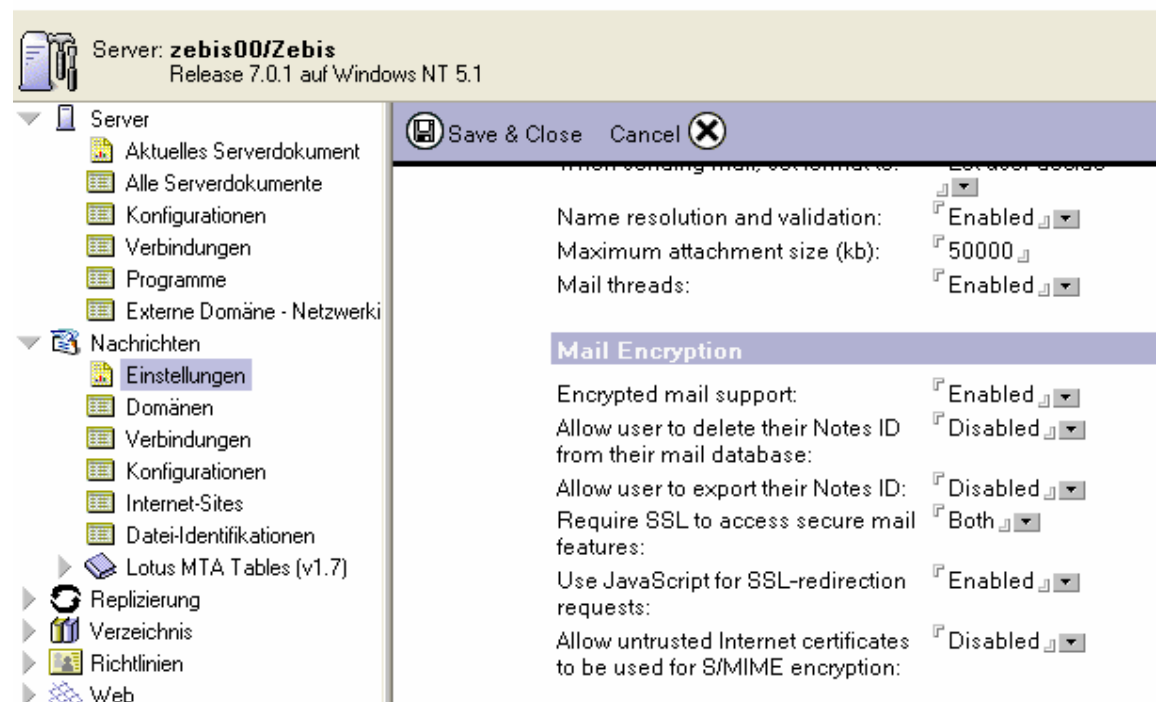
004 Browser Cache Management

Die Konfigurationsoptionen in diesem Bereich erlauben es, dass diese Browser Zusatzoption automatisch in jedem Browser installiert werden soll, über den ein Zugriff auf Domino Web Access erfolgt. Wenn sie diese Option wählen, dann wird bei dem ersten Domino Web Access Zugriff diese Komponenten von dem Domino Server in den Browser installiert. Alternativ dazu kann zwar auch angegeben werden, dass der Benutzer diese Option selbständig installieren darf – allerdings bietet sich dies wohl nicht wirklich an. Neben diesen Cache basierten Einstellungen können wir in diesem Bereich auch noch festlegen, ob der Anwender mittels Domino Web Access Dateianhänge, welche in einem Notes Dokument enthalten sind, öffnen und einsehen bzw. verarbeiten darf.

Mit der Angabe des „Default Cache Scrubbing Levels“ lässt sich steuern, welche der Teilbereiche von Notes Anwendungen aus dem Cache entfernt werden sollen. Dabei können sie zwischen den folgenden Einstellungsoptionen wählen:

- 0 – löscht alle persönlichen Maildatenbankdaten aus dem Cache Speicher
- 1 – Löscht alle Cache Einträge, die mit dem Mail Dateipfad beginnen
- 2 – Löscht alle Cache Einträge, welche den Host Namen des Domino Servers enthalten. Ausgenommen sind in diesem Fall Maskendateien
- 3 – dieser Wert verhält sich ähnlich wie der Wert „2“ mit dem Unterschied, dass in diesem Fall auch die Maskendateien mit entfernt werden
- 4 – löscht jeden Cache Inhalt. Ausgenommen sind die Maskendateien, die auf die iNotes Masken „/iNotes/Forms7“ und „/iNotes/Forms6“ verweisen.

Neben der Cache Verwaltung kann als weitere Sicherheitsaspekt der Einsatz von verschlüsselten Mails in Verbindung mit Domino Web Access erwägt werden. Diese Option kann ebenfalls in dem Domino Web Access Dokument konfiguriert werden. Wählen sie auch in diesem Fall in dem Navigationsbereich den Eintrag „Nachrichten / Einstellungen“ und selektieren sie anschließend den Tabellenbereich „Domino Web Access“. Dort finden sie unter anderem auch den Abschnitt „Mail Encryption“.



005 Mail Verschlüsselung

Wenn sie die Option „Encrypted mail support“ aktivieren, dann benötigen sie für den Zugriff auf Mails mit Domino Web Access eine Notes ID, die in der Mail-Datenbank gespeichert sein muss.

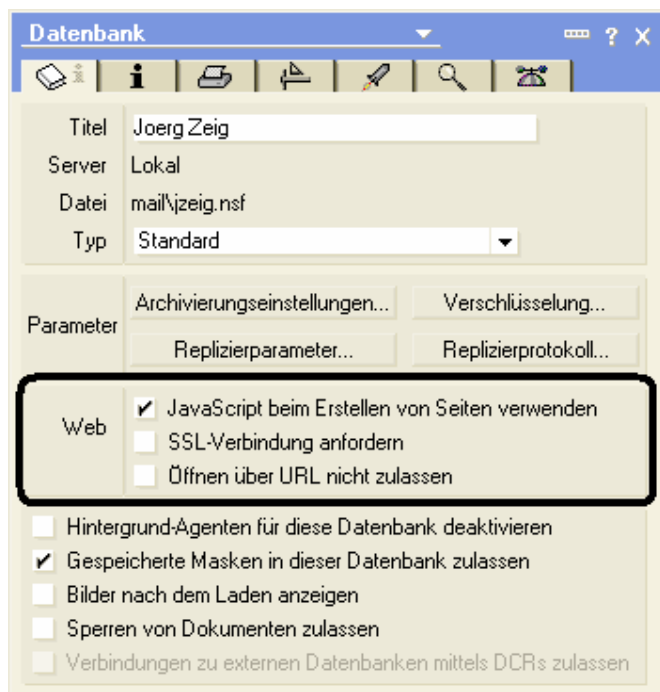
Mit der Option „Allow user to export their Notes ID“ legt fest, ob Benutzer die Notes ID in einer Datei speichern dürfen.

Eine weitere, sicherheitsrelevante Option ist die Möglichkeit, SSL Verschlüsselung bei dem Mail Verkehr anzuwenden. Hier können sie unter anderem wählen, ob diese Verschlüsselung nur für den Client, oder sowohl für den Client als auch den Server Gültigkeit hat. Die SSL Verschlüsselung wird per Standard über den Port 443 realisiert. Bei Bedarf können sie diese PortEinstellung jedoch auch abändern.

Eine solche SSL Verschlüsselung lässt sich außerdem wahlweise nur auf den Bereich der Authentifizierung verwenden, oder diese auch für die gesamte Verbindung – also auch für den Zugriff auf die Domino Daten – konfigurieren.

Bei der SSL Verschlüsselung läuft der gesamte Kommunikationspart über den https-Bereich. Generell ist ein Domino Server in der Lage, beide Protokolle gleichzeitig zu unterstützen.

Jede Datenbank, die auf einem Domino Server über das Internet genutzt werden soll (auch unabhängig von der Verwendung von Domino Web Access) sollte für diesen Zugriff zusätzlich abgesichert werden. Deshalb gilt als Empfehlung, Domino Datenbanken für eine Internet-basierte Nutzung entsprechend vorzubereiten. Diese Einstellungen lassen sich in den Datenbankeigenschaften der jeweiligen Domino Datenbank vornehmen. In einer solchen Datenbank wählen sie dazu die Menüoption „Datei / Datenbank / Eigenschaften“. Dort befindet sich auch der Abschnitt „Web“, indem sie unter anderem SSL Verbindungen anfordern können. Zusätzlich lässt sich dort auch das Öffnen dieser Domino Datenbank über eine URL Angabe unterbinden.



006 SSL Angaben in den Datenbankeigenschaften

Mit diesen Einstellungen lassen sich zwar die hohen Sicherheitsstandards eines Notes Clients nicht zu 100 % abbilden, sie bieten aber trotzdem eine weitestgehende Sicherheit gegen unberechtigte Zugriffe. Trotzdem ist es aber genau der Sicherheitsaspekt, der für oder wider den Einsatz von Domino Web Access sprechen könnte.